DOC 56 **1002/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

17 september 2025

WETSONTWERP

betreffende de weerbaarheid van kritieke entiteiten

Inhoud Blz.

OVEREENKOMSTIG ARTIKEL 8, § 2, 1°, VAN DE WET VAN 15 DECEMBER 2013 WERD DE IMPACTANALYSE NIET GEVRAAGD.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

17 septembre 2025

PROJET DE LOI

relatif à la résilience des entités critiques

Sommaire Pages

CONFORMÉMENT À L'ARTICLE 8, § 2, 1°, DE LA LOI DU 15 DÉCEMBRE 2013, L'ANALYSE D'IMPACT N'A PAS ÉTÉ DEMANDÉE.

01984

De regering heeft dit wetsontwerp op 17 september 2025 ingediend.	*Le gouvernement a déposé ce projet de loi le 17 septembre 2025.*
De "goedkeuring tot drukken" werd op 17 september 2025 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 17 septembre 2025.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*
ONAFH/INDÉP	:	*Onafhankelijk-Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

SAMENVATTING

Dit wetsontwerp voorziet in de omzetting van de Richtlijn 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (CER-Richtlijn). De CER-Richtlijn trekt de ECI-Richtlijn in, welke de rechtsbasis vormde voor de Belgische wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur. In het licht van het dynamische risicolandschap, volstond deze wetgeving niet meer om de kritieke entiteiten op voldoende wijze te beveiligen. Het wetsontwerp voorziet in een verderzetting van het kader dat werd gecreëerd door de wet van 2011, met de nodige toevoegingen op grond van de CER-Richtlijn. De Richtlijn creëert een overkoepelend en geharmoniseerd kader betreffende de weerbaarheid van kritieke entiteiten ten aanzien van alle gevaren: natuurrampen, incidenten die, accidenteel of opzettelijk, door de mens worden veroorzaakt, alsook noodsituaties op het gebied van volksgezondheid zoals pandemieën.

Deze wetgeving gaat om de organisatie van het nemen van weerbaarheidsmaatregelen door de kritieke entiteiten, en indien noodzakelijk, beschermingsmaatregelen door de bevoegde overheden, teneinde elk voorval dat van aard is om een aanzienlijk verstorend effect te hebben op de verlening van essentiële diensten door de kritieke entiteiten, te voorkomen of te verhinderen. In het geval een incident zich toch voordoet, poogt deze wetgeving de kritieke entiteiten op voorhand in staat te stellen de nodige maatregelen ter beschikking te hebben om zich hiertegen te verdedigen.

RÉSUMÉ

Ce projet de loi prévoit la transposition de la directive 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 relative à la résilience des entités critiques et abrogeant la directive 2008/114/CE du Conseil (directive CER). La directive CER remplace la directive ICE, qui constituait la base juridique de la loi belge du 1er juillet 2011 sur la sécurité et la protection des infrastructures critiques. Face à l'évolution dynamique des risques, cette législation ne suffisait plus à sécuriser efficacement les entités critiques. Le projet de loi s'inscrit dans le prolongement du cadre instauré par la loi de 2011 en y apportant les ajouts nécessaires conformément à la directive CER. La directive établit un cadre global et harmonisé en matière de résilience des entités critiques face à tous les types de dangers: catastrophes naturelles, incidents malveillants ou accidents d'origine humaine, ainsi que les urgences de santé publique telles que les pandémies.

Cette législation concerne l'organisation des mesures de résilience à prendre par les entités critiques et, si nécessaire, des mesures de protection à mettre en œuvre par les autorités compétentes, afin de prévenir ou d'empêcher tout incident susceptible de perturber significativement la prestation de services essentiels par ces entités critiques. En cas d'incident, cette législation vise à préparer les entités critiques à disposer à l'avance des mesures nécessaires pour y faire face.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Het voorliggend wetsontwerp zorgt voor de omzetting in Belgisch recht van de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG van de Raad (hierna te noemen "de CER-Richtlijn"). Zij heeft als doel de weerbaarheid te vergroten van kritieke entiteiten die diensten verlenen die essentieel zijn voor de vitale maatschappelijke functies of economische activiteiten op de interne markt.

De CER-Richtlijn beoogt de intrekking en vervanging van de Richtlijn 2008/114/EG van de Raad van 5 december 2008 inzake de identificatie en de aanduiding van Europese kritieke infrastructuren en de beoordeling van de noodzaak de beveiliging van dergelijke infrastructuren te verbeteren (ECI-Richtlijn). De ECI-Richtlijn was uitsluitend gericht op de beveiliging van Europese kritieke infrastructuren in de sectoren energie en transport, waarvan de ontwrichting of vernietiging aanzienlijke grensoverschrijdende gevolgen zou hebben voor ten minste twee lidstaten. Deze Richtlijn werd in Belgisch recht omgezet in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren (hierna de "KI-wet"). De KI-wet ging reeds verder dan wat de ECI-Richtlijn oplegde, daar op nationaal niveau niet enkel Europese kritieke infrastructuren werden geïdentificeerd, maar ook nationale kritieke infrastructuren. Het aantal sectoren dat onder het toepassingsgebied viel, werd tevens op grond van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid aanzienlijk uitgebreid op nationaal niveau met de sectoren drinkwater, ruimtevaart, gezondheidszorg, financiën, elektronische communicatie en digitale infrastructuren.

Na een evaluatie door de Europese Commissie van de ECI-Richtlijn in 2019, bleek dat door de steeds sterkere verwevenheid en grensoverschrijdende aard van activiteiten waarbij gebruik wordt gemaakt van kritieke infrastructuur, beschermende maatregelen met betrekking tot louter individuele activa niet volstaan om alle verstoringen te voorkomen. Er werd besloten dat een aanpak nodig was waarin meer oog was voor de risico's, waarin de rol en plichten van kritieke entiteiten die essentiële diensten aanbieden beter omschreven worden

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

Le présent projet de loi transpose en droit belge la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (dénommée ci-après "la directive CER"). Elle a pour objectif d'accroître la résilience des entités critiques qui fournissent des services essentiels pour les fonctions sociétales ou les activités économiques vitales dans le marché intérieur.

La directive CER vise à abroger et à remplacer la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (directive ICE). La directive ICE était exclusivement axée sur la protection des infrastructures critiques européennes dans les secteurs de l'énergie et des transports, dont l'arrêt ou la destruction aurait un impact transfrontalier significatif pour au moins deux États membres. Cette directive a été transposée en droit belge par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (ci-après la "loi IC"). La loi IC allait déjà plus loin que ce qu'imposait la directive ICE dans la mesure où non seulement des infrastructures critiques européennes étaient identifiées au niveau national, mais aussi des infrastructures critiques nationales. Le nombre de secteurs relevant du champ d'application a également été considérablement étendu à l'échelle nationale, sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, afin d'inclure les secteurs de l'eau potable, de l'espace, des soins de santé, de la finance, des communications électroniques et des infrastructures numériques.

À la suite d'une évaluation de la directive ICE par la Commission européenne en 2019, il s'est avéré qu'en raison de l'interconnexion et du caractère transfrontalier croissants des activités ayant recours aux infrastructures critiques, les mesures de protection relatives à des actifs purement individuels ne suffisent pas pour prévenir toutes les perturbations. Il a été décidé de la nécessité d'une approche qui tienne davantage compte des risques, dans laquelle le rôle et les obligations des entités critiques fournissant des services essentiels sont mieux définis

en samenhangend zijn, en waarin Unieregels worden vastgesteld om de weerbaarheid van kritieke entiteiten te vergroten.

Met de CER-Richtlijn wordt tegemoetgekomen aan de nood om kritieke entiteiten beter uit te rusten om het hoofd te bieden aan de risico's die de verlening van essentiele diensten zouden kunnen verstoren. Het dynamisch dreigingslandschap, met onder andere veranderende hybride en terroristische dreigingen, alsook de toenemende onderlinge afhankelijkheid tussen infrastructuren en sectoren, zorgt ervoor dat de ECI-Richtlijn niet meer volstaat om deze entiteiten voldoende te beschermen. Bovendien is er een toenemend risico wegens natuurrampen en klimaatverandering, waardoor zich vaker en op grotere schaal extreme weersomstandigheden zullen voordoen. De CER-Richtlijn creëert een overkoepelend en geharmoniseerd kader betreffende de weerbaarheid van kritieke entiteiten ten aanzien van alle gevaren, d.w.z. zowel natuurrampen als rampen die, accidenteel of opzettelijk, door de mens worden veroorzaakt, alsook noodsituaties op het gebied van volksgezondheid zoals pandemieën.

De CER-Richtlijn stelt geharmoniseerde minimumvoorschriften vast om de verlening van essentiële diensten op de interne markt te waarborgen in de gehele Unie. Het is mogelijk dat lidstaten bijkomende voorschriften opleggen, doch blijft het gelijke speelveld gewaarborgd door het feit dat elke lidstaat gehouden is aan eenzelfde kader van basis voorschriften.

Waar voorheen in de ECI-Richtlijn gesproken werd over "kritieke infrastructuren", gebruikt de CER-Richtlijn hoofdzakelijk het concept "kritieke entiteit". De CER-Richtlijn gaat namelijk uit van een inclusieve visie van de entiteiten die essentiële diensten verlenen, en waar voorheen enkel naar de infrastructuur gekeken werd, zal vanaf nu focus liggen op de hele entiteit. Een kritieke entiteit is "een publieke of particuliere entiteit die overeenkomstig de CER-wet is geïdentificeerd als behorende tot één van de categorieën die zijn vermeld in de tabel in bijlage." Om geïdentificeerd te kunnen worden als kritieke entiteit moet er aan drie voorwaarden voldaan worden, nl. de entiteit verleent essentiële diensten, de kritieke infrastructuur bevindt zich op het Belgisch grondgebied en een incident zou een aanzienlijk verstorend effect hebben op de verlening van die essentiële dienstverlening.

In dit ontwerp werd er gekozen om ook het concept van "kritieke infrastructuur" te behouden, naast het concept van "kritieke entiteit". Eén van de hoofdvoorwaarden om als kritieke entiteit aangeduid te kunnen worden, is nl. de voorwaarde dat een kritieke infrastructuur van de entiteit zich bevindt op Belgisch grondgebied. De CER-Richtlijn focust zich onder meer op

et sont cohérents, et qui prévoit des règles de l'Union destinées à renforcer la résilience des entités critiques.

La directive CER répond au besoin de mieux équiper les entités critiques afin de faire face aux risques susceptibles de perturber la fourniture de services essentiels. Le paysage dynamique des menaces, en ce compris l'évolution des menaces hybrides et terroristes, de même que l'interdépendance croissante entre les infrastructures et les secteurs, impliquent que la directive ICE ne suffisait plus pour protéger adéquatement ces entités. Force est en outre de constater un risque accru lié aux catastrophes naturelles et aux changements climatiques, qui va induire des phénomènes météorologiques extrêmes plus fréquents et à plus grande échelle. La directive CER crée un cadre global et harmonisé sur la résilience des entités critiques face à tous les dangers, à savoir tant les catastrophes naturelles que les catastrophes provoquées, de façon accidentelle ou intentionnelle, par l'homme, ainsi que les situations d'urgence en matière de santé publique, telles que les pandémies.

La directive CER établit des règles minimales harmonisées pour garantir la fourniture de services essentiels dans le marché intérieur dans toute l'Union. Les États membres peuvent imposer des règles supplémentaires, mais l'égalité des conditions de concurrence reste garantie par le fait que chaque État membre est lié par le même cadre de règles de base.

Si la directive ICE parlait "d'infrastructures critiques", la directive CER a principalement recours au concept d'"entité critique". La directive CER se base en effet sur une vision inclusive des entités qui fournissent des services essentiels et, alors que seule l'infrastructure était auparavant prise en compte, l'accent est désormais mis sur l'entité dans son ensemble. Une entité critique est "une entité publique ou privée identifiée, conformément à la loi CER, comme faisant partie d'une des catégories mentionnées dans le tableau en annexe." Afin de pouvoir être identifiée comme entité critique, trois conditions doivent être remplies, à savoir: l'entité fournit des services essentiels, l'infrastructure critique se situe sur le territoire belge et un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels.

Dans le présent projet, il a été décidé de maintenir également le concept d'"infrastructure critique", outre celui d'"entité critique". Une des conditions principales pour pouvoir être désignée comme entité critique est qu'une infrastructure critique de l'entité se situe sur le territoire belge. Etant donné que la directive CER met notamment l'accent sur la protection physique, il est

de fysieke bescherming, waardoor het opportuun is om beide concepten te hanteren aangezien er steeds fysieke kritieke infrastructuur aanwezig zal moeten zijn in de kritieke entiteit om als zodanig geïdentificeerd te worden. Bovendien is het zo dat niet elke infrastructuur van een kritieke entiteit dezelfde functie heeft en steeds essentiële diensten verleent, waardoor met het behouden van dit concept ook een duidelijk onderscheid kan gemaakt worden tussen niet-kritieke en kritieke infrastructuren van een kritieke entiteit, dewelke dan op gepaste wijze kunnen beschermd worden. Bovendien houdt de CER-Richtlijn in dat er zowel fysieke als organisatorische maatregelen genomen moeten worden, zoals bijvoorbeeld maatregelen die betrekking hebben op de bedrijfscontinuïteit. Deze maatregelen moeten op een passend niveau genomen kunnen worden in de kritieke entiteit. Fysieke beveiligingsmaatregelen zullen zowel op entiteit niveau als op het niveau van de infrastructuren moeten toegepast kunnen worden, terwijl organisatorische maatregelen eerder genomen zullen moeten worden op entiteit niveau. Het volstaat niet om enkel op entiteit niveau fysieke beveiligingsmaatregelen in te voeren wanneer de meest gevoelige plaatsen van de kritieke entiteit infrastructuren zijn die gelegen zijn op een andere locatie. Het onderscheid tussen kritieke entiteit en kritieke infrastructuur staat bijgevolg toe dat de verschillende soorten maatregelen in de praktijk op passend niveau genomen kunnen worden.

Kritieke entiteiten spelen als verleners van essentiële diensten een onmisbare rol bij het in stand houden van vitale maatschappelijke functies of economische activiteiten op de interne markt, in een economie die in de Europese Unie in toenemende mate onderling afhankelijk is. Het wetsontwerp heeft als doel te waken over het behoud en de weerbaarheid van vitale functies zoals onder andere de productie en transport van energie, de vitale vervoersinfrastructuren en -systemen, de onontbeerlijke schakels in het elektronische betalingsvervoer, de vitale verbindingen van elektronische communicatie, de onmisbare entiteiten in de gezondheidszorg en faciliteiten die ervoor zorgen dat burgers over drinkwater beschikken. Het wetsontwerp stelt een gemeenschappelijke benadering in werking, waarbij rekening wordt gehouden met het essentiële karakter van de sectoren waarop de CER-Richtlijn wordt toegepast, met name de sectoren: energie, vervoer, bankwezen, financiële marktinfrastructuur, digitale infrastructuur, drinkwater, afvalwater, volksgezondheid, overheidsinstellingen, ruimtevaart en voeding.

Deze wetgeving situeert zich hoofdzakelijk in het domein van de preventie. Het gaat om de organisatie van het nemen van weerbaarheidsmaatregelen door de kritieke entiteit, en indien noodzakelijk beschermingsmaatregelen door de bevoegde overheden, teneinde elk

opportun d'avoir recours aux deux concepts dans la mesure où il devra toujours y avoir une infrastructure critique physique dans l'entité critique pour pouvoir être identifiée comme telle. Par ailleurs, toutes les infrastructures d'une entité critique n'ayant pas la même fonction et ne fournissant pas toujours des services essentiels, le maintien de ce concept permet également de distinguer clairement les infrastructures non critiques des infrastructures critiques d'une entité critique, lesquelles peuvent alors être protégées de manière adéquate. En outre, la directive CER implique que des mesures tant physiques, qu'organisationnelles soient prises, telles que des mesures ayant trait à la continuité des activités. Ces mesures doivent pouvoir être prises à un niveau approprié de l'entité critique. Les mesures de sécurité physique devront s'appliquer tant au niveau de l'entité qu'au niveau de l'infrastructure, tandis que les mesures organisationnelles sont plus susceptibles de devoir être prises au niveau de l'entité. Il ne suffit pas de mettre en œuvre des mesures de sécurité physique uniquement au niveau de l'entité lorsque les sites les plus sensibles de l'entité critique sont des infrastructures situées sur un autre site. La distinction entre entité critique et infrastructure critique permet aux différents types de mesures d'être prises à un niveau approprié, dans la pratique.

En tant que fournisseurs de services essentiels, les entités critiques jouent un rôle indispensable dans le maintien des fonctions sociétales ou des activités économiques vitales sur le marché intérieur, dans une économie de plus en plus interdépendante au sein de l'Union européenne. Le projet de loi vise à veiller au maintien et à la résilience des fonctions vitales, entre autres la production et le transport d'énergie, les infrastructures et systèmes de transport vitaux, les maillons indispensables dans les moyens de paiements électroniques, les connexions vitales de communication électronique, les entités indispensables aux soins de santé et les installations qui permettent aux citoyens de disposer d'eau potable. Le projet de loi met en place une approche commune, qui tient compte du caractère essentiel des secteurs auxquels la directive CER s'applique, à savoir: l'énergie, les transports, le secteur bancaire, l'infrastructure des marchés financiers, l'infrastructure numérique, l'eau potable, les eaux usées, la santé publique, les institutions publiques, l'espace et l'alimentation.

Cette législation se situe principalement dans le domaine de la prévention. Il s'agit d'organiser la prise de mesures de résilience par l'entité critique et, si nécessaire, de mesures de protection par les autorités compétentes afin de prévenir ou d'empêcher tout événement de nature

voorval dat van aard is om een aanzienlijk verstorend effect te hebben op de verlening van essentiële diensten door de kritieke entiteit, te voorkomen of te verhinderen. In het geval een incident zich toch voordoet, poogt deze wetgeving de kritieke entiteiten de nodige tools te geven om zich hiertegen te beschermen. Kritieke entiteiten zullen echter wel een intern noodplan moeten opstellen, als onderdeel van hun weerbaarheidsplan van de kritieke entiteit (hierna: W.P.E.).

Dit wetsontwerp situeert zich verder niet in het raam van de voorbereiding op het beheer van een noodsituatie, waarvoor de ter zake reeds bestaande wettelijke en reglementaire bepalingen dienen te worden toegepast (wet van 31 december 1963 betreffende de civiele bescherming, *Belgisch Staatsblad*, 16 januari 1964; koninklijk besluit van 26 april 2024 tot vaststelling van het nationaal noodplan, *Belgisch Staatsblad* 14 mei 2024; wet van 15 mei 2007 betreffende de civiele veiligheid, *Belgisch Staatsblad* 31 juli 2007; koninklijk besluit van 22 mei 2019 betreffende de noodplanning en het beheer van noodsituaties op gemeentelijk en provinciaal niveau en betreffende de rol van de burgemeesters en de provinciegouverneurs in geval van crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen, *Belgisch Staatsblad* 27 juni 2019).

De Richtlijn legt de lidstaten de verplichting op om risicobeoordelingen uit te voeren met betrekking tot de sectoren die onder haar toepassingsgebied vallen. Het uitvoeren van deze sectorale risicobeoordeling valt onder de verantwoordelijkheid van de sectorale overheden, die bevoegd zijn voor hun welbepaalde (deel-)sectoren. Deze risicobeoordeling dient om de risico's per sector of deelsector te identificeren. Bij het uitvoeren van deze risicobeoordeling wordt tevens rekening gehouden met andere algemene of sectorspecifieke risicobeoordelingen die krachtens andere rechtshandelingen van de Unie zijn verricht, en moeten zij de onderlinge afhankelijkheid van sectoren in aanmerking nemen. De CER-Richtlijn verwijst hierbij ook naar de risicobeoordeling die is uitgevoerd overeenkomstig artikel 6, a), van Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad. Dit betreft de Belgische Nationale Risicobeoordeling, en wordt gecoördineerd door het NCCN. De high level resultaten hiervan worden gedeeld met de sectorale overheden zodat zij deze kunnen gebruiken bij het opstellen van hun eigen sectorale risicobeoordeling, alsook met de kritieke entiteiten zodat deze gebruikt kunnen worden bij het uitvoeren van hun risicobeoordeling en het opstellen van het W.P.E.

Vooraleer weerbaarheidsmaatregelen verplicht kunnen gesteld worden, dienen entiteiten geïdentificeerd te worden op basis van de bepalingen uit deze wet. Het is belangrijk te benadrukken dat de identificatie van

à perturber de manière significative la fourniture des services essentiels par l'entité critique. Au cas où un incident survient malgré tout, cette législation tente de fournir aux entités critiques les outils nécessaires pour s'en protéger. Toutefois, les entités critiques devront préparer un plan d'urgence interne dans le cadre de leur plan de résilience de l'entité critique (ci-après: P.R.E.).

Le présent projet de loi ne se situe pas davantage dans le cadre des préparatifs liés à la gestion d'une situation d'urgence. Le cas échéant, les dispositions légales et réglementaires existantes doivent être appliquées (loi du 31 décembre 1963 relative à la protection civile, *Moniteur belge*, 16 janvier 1964; arrêté royal du 26 mai 2024portant fixation du plan d'urgence national, *Moniteur belge*, 14 mai 2024; Loi du 15 mai 2007 relative à la sécurité civile, *Moniteur belge* 31 juillet 2007; arrêté Royal du 22 mai 2019 relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial et au rôle des bourgmestres et des gouverneurs de province en cas d'événements et de situations de crise nécessitant une coordination ou une gestion à l'échelon national, *Moniteur belge* 27 juin 2019).

La directive oblige les États membres à effectuer des évaluations de risques concernant les secteurs qui relèvent de son champ d'application. La réalisation de ces évaluations sectorielles de risques relève de la responsabilité des autorités sectorielles, qui sont compétentes pour leurs (sous-)secteurs bien précis. Cette évaluation de risques sert à identifier les risques par secteur et sous-secteur. Dans le cadre de la réalisation de ces évaluations des risques, il est également tenu compte d'autres évaluations de risques générales ou sectorielles qui ont été effectuées en vertu d'autres actes juridiques de l'Union, et l'interdépendance des secteurs doit être prise en compte. La directive CER fait également référence ici à l'évaluation des risques réalisée conformément à l'article 6, a), de la décision n° 1313/2013/UE du Parlement européen et du Conseil. Ceci concerne l'évaluation nationale belge des risques, coordonnée par le NCCN. Les résultats de haut niveau de ces évaluations seront partagés avec les autorités sectorielles afin qu'elles puissent les utiliser pour préparer leur propre évaluation des risques sectoriels, ainsi qu'avec les entités critiques afin qu'elles puissent les utiliser lors de l'évaluation des risques et de la préparation du P.R.E.

Avant de pouvoir prendre des mesures obligatoires de résilience, les entités doivent être identifiées sur la base des dispositions de la présente loi. Il est important de souligner que l'identification des entités critiques ne se

kritieke entiteiten niet gebeurt op basis van de sectorale risicobeoordeling, maar op basis van een impactanalyse, waar men onder meer rekening moet houden met de risico's geïdentificeerd in de sectorale risicobeoordeling.

Deze opdracht is toevertrouwd aan de sectorale overheid, met name de overheid die bevoegd is voor een welbepaalde sector of deelsector. De sectorale overheden werken samen met de vertegenwoordigers van de sector en zelfs met de potentiële kritieke entiteiten, aangezien ze samen over de nodige expertise beschikken met betrekking tot hun welbepaalde sector. De KI-wet introduceerde het concept van sectorale overheid, en de manier van identificatie uit de KI-wet wordt overgenomen in dit wetsontwerp mits de noodzakelijke aanpassingen gelet op de CER-Richtlijn, aangezien de sectorale overheden vertrouwd zijn met de procedure en zij het best geplaatst zijn om deze identificatie en aanduiding uit te voeren. Gelet op het feit dat er onder het toepassingsgebied van dit voorstel een aantal sectoren, zoals de drinkwater en afvalwater sector, onder het toepassingsgebied vallen waarvoor de bevoegdheid in België verdeeld werd tussen de federale en gefedereerde entiteiten, voeren de bevoegde federale overheden deze functie uit samen met de gefedereerde entiteiten voor zover de kritieke entiteiten onder hun bevoegdheden vallen. Daarna is het de taak voor de sectorale overheden om de kritieke entiteiten te gaan identificeren en aanduiden. Deze aanduiding is van belang omdat deze ervoor zorgt dat de verplichtingen uit deze wet op die entiteiten van toepassing zullen zijn.

Hierdoor is het dus mogelijk dat de omzetting van de CER-Richtlijn ook een impact heeft op sectoren die tot de bevoegdheid van de gefedereerde entiteiten behoren. Dit was echter reeds het geval bij de omzetting van de ECI-Richtlijn. In haar advies betreffende de KI-wet stelde de Raad van State dat maatregelen die op basis van het voorontwerp zullen worden getroffen, "een weerslag zouden kunnen hebben op operatoren die een infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid *ratione materiae* van de gewesten kan behoren, waardoor werd aanvaard dat zij werden betrokken in het proces omschreven in de wet". Daarnaast werd gesteld dat dit eveneens zou kunnen gelden voor andere sectoren waarop de KI-wet toepassing zou vinden (adv. RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuur en andere punten van federaal belang, *Parl. St.* Kamer 2010-11, nr. DOC 53 1357/001, 55).

De Raad van State heeft dit advies in 2019 bevestigd in 2019 in het kader van de goedkeuring van de NIS-wet. Deze wet heeft het toepassingsgebied van de KI-wet uitgebreid naar meer sectoren , waaronder sectoren

fait pas sur la base de l'évaluation des risques sectoriels, mais sur la base d'une analyse d'impact, dans laquelle il faut tenir compte, entre autres, des risques identifiés dans l'évaluation des risques sectoriels.

Cette mission est confiée aux autorités sectorielles, à savoir les autorités compétentes pour un secteur ou sous-secteur déterminé. Les autorités sectorielles collaborent avec les représentants du secteur, voire avec les entités critiques potentielles étant donné qu'elles disposent ensemble de l'expertise nécessaire concernant leur secteur déterminé. La loi IC a introduit le concept d'autorité sectorielle et le mode d'identification de la loi IC est repris dans le présent projet de loi, moyennant les ajustements nécessaires compte tenu de la directive CER, étant donné que les autorités sectorielles sont familiarisées avec la procédure et qu'elles sont les mieux placées pour effectuer cette identification et cette désignation. Dans la mesure où le champ d'application de ce projet vise toute une série de secteurs, comme celui de l'eau potable ou du traitement des eaux résiduaires dont la compétence a été répartie en Belgique entre les entités fédérales et fédérées, les autorités fédérales compétentes remplissent cette fonction en collaboration avec les entités fédérées dans la mesure où les entités critiques relèvent de leurs compétences. Il revient par ailleurs aux autorités sectorielles d'identifier et de désigner les entités critiques. Cette désignation est importante parce qu'elle garantit que les obligations prévues par la présente loi s'appliqueront à ces entités.

Il est donc possible que la transposition de la directive CER ait également un impact sur les secteurs relevant de la compétence des entités fédérées. Toutefois, cela était déjà le cas lors de la transposition de la directive ICE. Dans son avis sur la loi ICE, le Conseil d'État avait indiqué que les mesures à prendre sur la base de l'avant-projet "pourraient affecter les opérateurs exploitant des infrastructures qui, d'un autre point de vue, peuvent relever de la compétence *ratione materiae* des régions, de sorte qu'il a été admis qu'elles soient incluses dans le processus décrit dans la loi". En outre, il a été indiqué que cela pourrait également s'appliquer à d'autres secteurs auxquels la loi IC s'appliquerait (avis C.E. 48.989/VR du 9 décembre 2010 sur un avant-projet de loi concernant les infrastructures critiques, les autres points d'intérêt fédéral et les points d'intérêt local, *Doc. Parl.*, Chambre, 2010-2011, n° DOC 53 1357/001, p. 55).

Le Conseil d'État a récemment confirmé cet avis en 2019 dans le cadre de l'adoption de la loi NIS. Cette loi a étendu le champ d'application de la loi IC à un plus grand nombre de secteurs, y compris des secteurs qui

die (deels) onder de bevoegdheid van de gefedereerde entiteiten vallen (de NIS-wet betrof naast de sectoren energie en transport ook onder meer de sectoren drinkwater, elektronische communicatie, gezondheidszorg, digitale infrastructuren en financiële marktinfrastructuren; adv. RvS nr. 63.296/4 van 2 mei 2018 over een voorontwerp van wet tot vaststelling van een kader voor de beveiliging van network- en informatiesystemen van algemeen belang voor de openbare veiligheid, *Parl. St.* Kamer 2018-19, nr. DOC 54 3340/001, 75-79). De Raad van State stelde in dit advies dat er voldoende rekening werd gehouden met de bevoegdheden van de gefedereerde entiteiten aangezien de gewesten betrokken werden bij de uitvoering van het voorontwerp (adv. RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuur en andere punten van federaal belang, *Parl. St.* Kamer 2010-11, nr. DOC 53 1357/001, 54). De gefedereerde entiteiten zullen dan ook betrokken worden bij de uitvoering van het huidige ontwerp van wet. Tijdens de identificatieprocedure zullen aldus de gefedereerde entiteiten steeds betrokken kunnen worden, zoals dat op basis van de huidige wetgeving reeds het geval is. Op deze manier wordt autonomie van de verschillende beleidsniveaus in acht genomen, aangezien de medewerking facultatief is en zulks niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen kan nemen.

De Raad van State heeft bovenstaand standpunt opnieuw bevestigd in hun advies over de voorliggende wet betreffende de weerbaarheid van kritieke entiteiten (adv. RvS nr. 76.573/2/V van 12 augustus 2024 over een voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten, 43) Volgens dit advies levert het voorontwerp geen bevoegdheidsproblemen op.

Een breed inzicht in de mogelijke risico's die de verlening van hun essentiële diensten kunnen verstoren, is noodzakelijk om de betrokken kritieke entiteiten hiertegen op adequate wijze weerbaar te maken. Bijgevolg zullen ook de kritieke entiteiten zelf, minstens elke 4 jaar, een risicobeoordeling moeten uitvoeren. Op basis daarvan nemen zij technische, beveiligings-, en organisatorische maatregelen die gepast en evenredig zijn gelet op de risico's waarmee zij geconfronteerd worden, om incidenten te voorkomen, te beperken of te beheersen, en om bescherming te bieden of bestand te zijn ertegen, te reageren erop of daarvan te herstellen. Deze maatregelen moeten worden vastgelegd in het W.P.E. Het W.P.E. mag bestaan uit plannen waarover de kritieke entiteit reeds beschikt op basis van andere wetgeving, zolang alle elementen die door de CER-Richtlijn worden opgelegd er maar in vervat werden.

In het kader van de weerbaarheid van kritieke entiteiten, wordt er een delegatie gegeven aan de Koning om de

relèvent (en partie) de la compétence des entités fédérées (outre les secteurs de l'énergie et des transports, la loi NIS couvre également les secteurs de l'eau potable, des communications électroniques, de la santé, des infrastructures numériques et des infrastructures des marchés financiers, entre autres; avis C.E. n° 63.296/4 du 2 mai 2018 sur un avant-projet de loi établissant un cadre pour la sécurité des systèmes de réseaux et d'information d'intérêt général de sécurité publique, *Doc. Parl.*, Chambre, 2018-2019, n° DOC 54 3340/001, p. 75-79). Dans cet avis, le Conseil d'État indique que les compétences des entités fédérées ont été suffisamment prises en compte puisque les régions ont été impliquées dans la mise en œuvre de l'avant-projet (avis C.E. n° 48.989/VR du 9 décembre 2010 sur un avant-projet de loi sur les infrastructures critiques et autres points d'intérêt fédéral, *Doc. Parl.*, Chambre, 2010-2011, n° DOC 53 1357/001, p. 54). Les entités fédérées seront donc associées à la mise en œuvre du présent projet de loi. Ainsi, lors de la procédure d'identification, les entités fédérées pourront toujours être impliquées, comme cela est déjà le cas sur la base de la législation actuelle. De cette manière, l'autonomie des différents niveaux politiques est respectée, puisque la coopération est facultative et que cela n'empêche pas le gouvernement fédéral compétent de prendre les mesures envisagées.

Le Conseil d'État a confirmé cette position dans l'avis sur la présente loi relative à la résilience des entités critiques (avis C.E. n° 76.573/2/V du 12 août 2024 sur un avant-projet de loi relative à la résilience des entités critiques, 43). Selon cet avis, l'avant-projet ne soulève pas de questions de compétence.

Une vaste compréhension des risques susceptibles de perturber la fourniture de leurs services essentiels est nécessaire pour que les entités critiques concernées puissent s'en prémunir de manière adéquate. C'est pourquoi les entités critiques devront elles-mêmes effectuer une évaluation des risques au moins tous les 4 ans. Sur cette base, elles prennent des mesures techniques, de sécurisation et organisationnelles qui sont appropriées et proportionnelles aux risques auxquels elles sont confrontées, afin de prévenir, de limiter ou de maîtriser les incidents et de s'en prémunir, d'y réagir ou de s'en rétablir. Ces mesures doivent être définies dans le P.R.E. Le P.R.E. peut être constitué de plans déjà à la disposition de l'entité critique en vertu d'autres législations, pour autant que tous les éléments requis par la directive CER y aient été inclus.

Dans le cadre de la résilience des entités critiques, une délégation au Roi est prévue pour désigner l'autorité

nationale autoriteit aan te duiden die belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit die deze rol vandaag al vervult en ook zal blijven vervullen is het Nationaal Crisiscentrum (hierna: NCCN). Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en op Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.

Het NCCN is verantwoordelijk voor de coördinatie met de politie-en veiligheidsdiensten, en kan extra maatregelen opleggen ter bescherming van de kritieke entiteiten wanneer nodig. Daarnaast ondersteunt het NCCN de sectorale overheden tijdens de identificatie-procedure van de kritieke entiteiten. Tevens verleent het NCCN een advies aan de sectorale overheden over het identificatiedossier van een kritieke entiteit, waarbij gewaarborgd wordt dat de criteria en drempelwaarden correct worden toegepast. Het NCCN vraagt ten slotte ook de dreigingsanalyses aan bij het OCAD, dewelke opgesteld worden voor elke sector of deelsector.

De KI-wet maakt nog een onderscheid tussen nationale kritieke infrastructuur en Europese Infrastructuur (hierna "EKI"), waarbij EKI werden gedefinieerd als zijnde "de nationale kritieke infrastructuur waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in ten minste twee lidstaten van de Europese Unie zou hebben of de kritieke infrastructuur die niet gelegen is op het Belgische grondgebied, maar op het grondgebied van een andere lidstaat van de Europese Unie, waarvan de onderbreking van de werking of de vernietiging een aanzienlijke weerslag zou hebben in ten minste twee lidstaten van de Europese Unie, waaronder België". Deze categorie werd niet hernomen in de CER-Richtlijn. Echter wordt, gelet op de onderlinge afhankelijkheid en mogelijkheid tot grensoverschrijdende gevolgen, bijzondere aandacht gegeven aan kritieke entiteiten die essentiële diensten verlenen aan of in meer dan 6 lidstaten. De CER-Richtlijn legt aan deze entiteiten een apart statuut op van "Kritieke Entiteit van Bijzonder Europees Belang". De Commissie kan in dergelijk geval adviesmissies organiseren om de door die entiteit genomen weerbaarheidsmaatregelen te beoordelen. Gevolg is dat de kritieke entiteiten die in andere lidstaten essentiële diensten verlenen, maar niet aan de drempel van zes of meer lidstaten voldoen, in dit ontwerp geen speciaal statuut meer kunnen krijgen. Het spreekt voor zich dat het nog steeds mogelijk is om een bilaterale

nationale chargée de la supervision et de la coordination de la mise en œuvre de cette loi.

L'autorité qui remplit déjà et continuera à remplir ce rôle aujourd'hui est le Centre de Crise National (ci-après: NCCN). Elle n'est pas directement mentionnée dans la loi car, comme l'a déjà relevé la section de législation du Conseil d'État, notamment dans son avis 63.296/4, désigner directement les services de l'exécutif mis en place par le Roi et nommés auprès de lui serait une ingérence du pouvoir législatif dans l'organisation interne de l'exécutif.

Le NCCN est responsable de la coordination avec les services de police et de sécurité, et peut, si nécessaire, imposer des mesures supplémentaires pour protéger les entités critiques. En outre, le NCCN soutient les autorités sectorielles au cours de la procédure d'identification des entités critiques. Le NCCN conseille également les autorités sectorielles sur le dossier d'identification d'une entité critique, en veillant à ce que les critères et les seuils soient correctement appliqués. Enfin, le NCCN demande également à l'OCAD des évaluations de la menace, qui sont établies pour chaque secteur ou sous-secteur.

La loi IC établit une autre distinction entre les infrastructures critiques nationales et les infrastructures critiques européennes (ci-après dénommées: "ICE"). Les ICE étaient définies comme étant "les infrastructures critiques nationales dont la perturbation du fonctionnement ou la destruction aurait un impact important dans au moins deux États membres de l'Union européenne, ou les infrastructures critiques qui ne sont pas situées sur le territoire belge, mais sur le territoire d'un autre État membre de l'Union européenne, dont la perturbation du fonctionnement ou la destruction aurait un impact important dans au moins deux États membres de l'Union européenne, y compris la Belgique." Cette catégorie n'est pas reprise dans la directive CER. Toutefois, compte tenu de l'interdépendance et de la possibilité de répercussions transfrontalières, une attention particulière est accordée, aux entités critiques qui fournissent des services essentiels à six États membres ou plus. La directive CER impose à ces entités un statut distinct d'"entité critique revêtant une importance européenne particulière". Le cas échéant, la Commission peut organiser des missions consultatives pour évaluer les mesures de résilience prises par cette entité. Par conséquent, les entités critiques qui fournissent des services essentiels dans d'autres États membres, mais qui n'atteignent pas le seuil de six États membres ou plus, ne peuvent plus bénéficier d'un statut spécial en vertu de ce projet. Bien

of multilaterale samenwerking op te richten. De CER-Richtlijn benadrukt deze mogelijkheid ook in artikel 11.

De kritieke entiteit zal een weerbaarheidsplan moeten opstellen, met daarin de weerbaarheidsmaatregelen die de entiteit neemt om tegemoet te komen aan de risico's waaraan zij blootgesteld kan worden, dewelke zij onderzocht heeft in haar risicobeoordeling. De kritieke entiteit zelf is steeds in de eerste plaats verantwoordelijk om haar eigen weerbaarheid te waarborgen alsook dat van haar infrastructuren. Haar rol is dus essentieel voor het voorkomen van en het weerbaar zijn tegen elke gebeurtenis die van aard is om een verstoring van de werking of de vernietiging van haar structuur met zich mee te brengen. Naast de weerbaarheidsmaatregelen, die intern in de entiteit genomen en uitgevoerd moeten worden, bestaan er ook externe beschermingsmaatregelen, dewelke door de bevoegde autoriteiten kunnen genomen worden.

De vermelding in deze wet van deze externe beschermingsmaatregelen is niet noodzakelijk aangezien deze hun wettelijke basis gekregen hebben in artikelen 7/1 tot 7/3, 14 en 17 van de wet op het politieambt van 5 augustus 1992, en artikelen 61, 62 en 97, eerste lid, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Bijgevolg bestaat de mogelijkheid tot externe beschermingsmaatregelen ongeacht of dit in de huidige wet wordt hernomen. Om de inhoud van de wet niet onnodig te verzwaren en om herhaling te voorkomen, werd ervoor gekozen om de bepalingen betreffende de externe beschermingsmaatregelen niet opnieuw op te nemen in het voorliggende ontwerp.

Het NCCN is bevoegd om in functie van het type dreiging externe beschermingsmaatregelen ten aanzien van kritieke entiteiten te nemen, hetzij op basis van een dreigingsanalyse zoals bedoeld in artikel 8, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, op haar verzoek of ambtshalve uitgevoerd door het OCAD, hetzij op basis van een analyse uitgevoerd door de diensten van de federale politie of de inlichtingen- en veiligheidsdiensten voor de andere dreigingen dan die bedoeld in artikel 3 van de voormelde wet en die onder hun bevoegdheid vallen. De externe beschermingsmaatregelen staan los van de weerbaarheidsmaatregelen die op grond van deze wet genomen moeten worden.

De burgemeester, die als eerste verantwoordelijk is voor de veiligheid op het grondgebied van zijn gemeente, kan welteverstaan ertoe worden gebracht externe beschermingsmaatregelen te moeten nemen, mits deze niet strijdig zijn met die waartoe het NCCN heeft beslist.

entendu, il est toujours possible d'établir une coopération bilatérale ou multilatérale. La directive CER souligne également cette possibilité à l'article 11.

L'entité critique devra élaborer un plan de résilience contenant les mesures de résilience qu'elle adopte pour faire face aux risques auxquels elle peut être confrontée et qu'elle a examinés dans le cadre de son évaluation des risques. L'entité critique est toujours chargée en premier lieu de garantir sa propre résilience et celle de ses infrastructures. Son rôle est donc essentiel pour prévenir et pour résister à tout événement de nature à entraîner une interruption du fonctionnement ou la destruction de sa structure. Outre les mesures de résilience qui doivent être prises et mises en œuvre au sein même de l'entité, il existe des mesures de protection externes que les autorités compétentes peuvent adopter.

La mention de ces mesures de protection externes dans la présente loi n'est pas nécessaire étant donné que leur base légale figure dans les articles 7/1 à 7/3, 14 et 17 de la loi du 5 août 1992 sur la fonction de police, et sur les articles 61, 62 et 97, alinéa 1er, de la loi du 7 décembre 1998 organisant un service de police intégré et structuré à deux niveaux. Par conséquent, la possibilité de mesures de protection externes existe indépendamment du fait qu'elle soit reprise dans la loi actuelle. Afin de ne pas alourdir inutilement le contenu de la loi et d'éviter les répétitions, il a été choisi de ne pas reproduire les dispositions relatives aux mesures de protection externes dans le présent projet.

Le NCCN est autorisé à prendre des mesures de protection externes à l'égard des entités critiques, en fonction du type de menace, soit sur la base d'une analyse de la menace visée à l'article 8, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, effectuée à sa demande ou d'office par l'OCAM, soit sur la base d'une analyse effectuée par les services de la police fédérale ou les services de renseignement et de sécurité pour les menaces autres que celles visées à l'article 3 de la loi précitée et relevant de leur compétence. Les mesures de protection externes sont distinctes des mesures de résilience à prendre en vertu de cette loi.

Le bourgmestre, qui est le premier responsable de la sécurité sur le territoire de sa commune, peut être amené à prendre des mesures de protection externes, pour autant qu'elles ne soient pas contraires à celles décidées par le NCCN.

Om te zorgen voor een integrale aanpak betreffende de weerbaarheid van kritieke entiteiten moet elke lidstaat tevens beschikken over een Strategie om de weerbaarheid van kritieke entiteiten te versterken. De strategie wordt opgesteld door het NCCN, op basis van input van de sectorale overheden, moet de uit te voeren strategische doelstellingen en beleidsmaatregelen bevatten, en wordt meegedeeld aan de Commissie. Deze strategie zal de realiteit beschrijven van het beleid dat gevoerd wordt betreffende de weerbaarheid van kritieke entiteiten.

De CER-Richtlijn is niet van toepassing op aangelegenheden die vallen onder Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad (hierna "NIS 2 Richtlijn"). Echter, gelet op het belang van cyberbeveiliging voor de weerbaarheid van kritieke entiteiten en met het oog op consistentie, werd in dit wetsvoorstel gezorgd voor een aanpak die coherent is met zowel de CER-Richtlijn als met de NIS 2-Richtlijn. Gezien de hogere frequentie en bijzondere kenmerken van cyberrisico's legt de NIS 2-Richtlijn een grote groep entiteiten brede voorschriften op om hun weerbaarheid te waarborgen. Gelet op de grote mate van verwevenheid van fysieke infrastructuur en cyber infrastructuur, kunnen deze twee wetgevende kaders niet los gezien worden van elkaar. Daarnaast zullen kritieke entiteiten die geïdentificeerd worden op grond van deze wet, van rechtswege essentiële entiteiten worden onder de NIS 2-Richtlijn, waardoor een goede samenwerking en vlotte informatie-uitwisseling met het Centrum voor Cybersecurity België in dit kader belangrijk is.

Het Unierecht legt financiële entiteiten en digitale infrastructuur entiteiten vergaande voorschriften op om alle risico's waarmee zij te maken krijgen, te beheersen en bedrijfscontinuïteit te waarborgen (Verordeningen (EU) nr. 648/2012, (EU) nr. 575/2013, (EU) nr. 600/2014 van het Europees parlement en de Raad en Richtlijnen 2013/36/EU en 2014/65/EU van het Europees Parlement en de Raad, recent aangevuld met Verordening (EU) 2022/2554 van het Europees Parlement en de Raad). Dit specifieke regime voor de sectoren van de digitale infrastructuur, de financiële marktinfrastructuur en het bankwezen heeft als gevolg dat de CER-Richtlijn bepaalt dat de verplichtingen vastgelegd in artikel 11 en de hoofdstukken III, IV en VI niet van toepassing zijn op entiteiten die behoren tot deze sectoren.

Men zal opmerken dat dit ontwerp de openbare veiligheid betreft en dus onder de bevoegdheid van de Federale Staat valt. In het federale België is het beleidsdomein veiligheid en ordehandhaving een quasi-integraal federale materie. Zo is de federale overheid op basis van haar residuaire bevoegdheid voor de preventieve bescherming

Afin de veiller à une approche intégrale de la résilience des entités critiques, chaque État membre doit également disposer d'une Stratégie visant à renforcer la résilience des entités critiques. La stratégie est établie par le NCCN, sur la base des contributions des autorités sectorielles, doit contenir les objectifs stratégiques et les mesures à mettre en œuvre et est communiquée à la Commission. Cette stratégie décrira la réalité des politiques menées en matière de résilience des entités critiques.

La directive CER ne s'applique pas aux matières couvertes par la directive (UE) 2022/2555 du Parlement européen et du Conseil (ci-après "directive NIS 2"). Toutefois, vu l'importance de la cybersécurité pour la résilience des entités critiques et par souci de cohérence, le présent projet de loi prévoit une approche qui est en cohérence tant avec la directive CER qu'avec la directive NIS 2. Étant donné la fréquence accrue et les particularités des cyber-risques, la directive NIS 2 impose à un grand groupe d'entités des règles étendues afin de garantir leur résilience. Vu le degré élevé d'interconnexion entre une infrastructure physique et une infrastructure cybernétique, ces deux cadres législatifs ne peuvent être dissociés. En outre, les entités critiques identifiées sur la base de la présente loi deviendront de plein droit des entités essentielles conformément à la directive NIS 2. Dans ce contexte, une bonne collaboration et un échange fluide d'informations avec le Centre pour la Cybersécurité Belgique sont donc importants.

Le droit de l'Union impose aux entités financières et aux infrastructures digitales des prescriptions poussées afin de maîtriser tous les risques auxquels elles sont confrontées et de garantir la continuité de leurs activités (règlements (UE) n° 648/2012, (UE) n° 575/2013, (UE) n° 600/2014 du Parlement européen et du Conseil, et directives 2013/36/UE et 2014/65/UE du Parlement européen et du Conseil, récemment complétées par le règlement (UE) 2022/2554 du Parlement européen et du Conseil). En raison de ce régime spécifique pour les secteurs de l'infrastructure numérique, de l'infrastructure des marchés financiers et le secteur bancaire, la directive CER stipule que les obligations prévues à l'article 11 et aux chapitres III, IV et VI ne s'appliquent pas aux entités qui relèvent de ces secteurs.

On remarquera que ce projet porte sur la sécurité publique et relève dès lors de la compétence de l'État fédéral. Dans la Belgique fédérale, le domaine politique de la sécurité et de l'ordre public est quasi intégralement une matière fédérale. Le gouvernement fédéral est ainsi responsable de la sécurité des infrastructures

op het gebied van openbare veiligheid bevoegd voor de beveiliging van kritieke infrastructuren.

In haar advies betreffende de KI-wet oordeelde de Raad van State dat “de omzetting van de ECI-Richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort” (zie o.m. adv. RvS nr. 38.278/AV van 16 mei 2006 over een voorstel van decreet houdende wijziging en aanvulling van het decreet van 28 februari 2003 betreffende het Vlaamse inburgeringsbeleid met een hoofdstuk VIII houdende het verbieden van het dragen van gelaatsverhullende gewaden, doorgaans aangeduid als “boerka”, *Parl. St.* Vl. Parl. 2004-05, nr. 159/2, 10; adv. RvS nr. 44.771/3 van 15 juli 2008 over een ontwerp van besluit van de Vlaamse regering houdende de normen voor de preventie van brand in de voorzieningen voor kinderopvang, 3; adv. RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuren, de andere punten van federaal belang en de punten van lokaal belang, *Parl. St.* Kamer 2010-11, nr. DOC 53 1357/001, 54; adv. RvS nr. 48.989/VR, 53-54; adv. RvS nr. 63.296/4 van 2 mei 2018 over een voorontwerp van wet tot vaststelling van een kader voor de beveiliging van network- en informatiesystemen van algemeen belang voor de openbare veiligheid, *Parl. St.* Kamer 2018-19, nr. DOC 54 3340/001, 75-79; K. REYBROUCK en S. SOTTIAUX, De federale bevoegdheden, 254-259). Naast de algemene preventieve bescherming van kritieke infrastructuren, is de federale overheid ook residuair bevoegd voor de strijd tegen radicalisme, extremisme, terrorisme en de bescherming van de infrastructuur tegen terroristische aanslagen (adv. RvS nr. 57.106/VR/3, 27-28; adv. RvS nr. 64.489/3 van 22 november 2018 over een voorontwerp van decreet van de Vlaamse Gemeenschap houdende instemming met het verdrag van de Raad van Europa ter voorkoming van terrorisme, gedaan te Warschau op 16 mei 2005, *Parl. St.* Vl. Parl. 2018-2019, nr. 1796/1, 17-18). De bevoegdheid van de federale overheid gaat dus verder dan het louter beschermen van kritieke infrastructuren tegen terroristische aanslagen. Het gaat om een algemene preventieve beschermingsbevoegdheid.

De nieuwe CER-Richtlijn herneemt deze “alle-risico’s aanpak”, zonder enige prioritering tussen de soorten dreigingen, aangezien er sprake is van een dynamisch dreigingslandschap. Het is duidelijk dat beide richtlijnen uitgaan van eenzelfde “alle-risico’s aanpak” al werd er in de huidige ECI-Richtlijn voorrang gegeven aan de bestrijding van terroristische dreigingen. De omzetting van de CER-Richtlijn valt daarom eveneens onder de

critiques sur la base de sa compétence résiduelle en matière de protection préventive dans le domaine de la sécurité publique.

Dans son avis sur la loi IC, le Conseil d’État a considéré que “la transposition de la directive ICE conduit essentiellement à la mise en œuvre de la matière de la protection préventive dans le domaine de la sécurité publique, qui relève de la compétence résiduelle exclusive du législateur fédéral” (voir e.a.: avis C.E., n° 38.278/AV du 16 mai 2006 sur une proposition de décret modifiant et complétant le décret du 28 février 2003 relatif à la politique flamande d’intégration par un chapitre VIII interdisant le port de robes dissimulant le visage, communément appelées “burka”, *Doc. Parl.*, Parl. Fl., 2004-2005, n° 159/2, 10; avis C.E. n° 44.771/3 du 15 juillet 2008 relatif à un projet d’arrêté du gouvernement Flamand contenant les normes de prévention des incendies dans les structures d’accueil pour enfants, 3; avis C.E. n° 48.989/VR du 9 décembre 2010 sur un avant-projet de loi sur les infrastructures critiques et autres points d’intérêt fédéral, *Doc. Parl.*, Chambre 2010-2011, n° DOC 53 1357/001, 54; Avis C.E. n° 63.296/4 du 2 mai 2018 sur un avant-projet de loi établissant un cadre pour la sécurité des systèmes de réseaux et d’information d’intérêt général de sécurité publique, *Doc. Parl.*, Chambre, 2018-2019, n° DOC 54 3340/001, p. 75-79; K. REYBROUCK et S. SOTTIAUX, De federale bevoegdheden, p. 254-259). Outre la protection préventive générale des infrastructures critiques, le gouvernement fédéral dispose également d’une compétence résiduelle en matière de lutte contre le radicalisme, l’extrémisme, le terrorisme et la protection des infrastructures contre les attaques terroristes (avis C.E., n° 57.106/VR/3, 27-28; avis C.E., n° 64.489/3 du 22 novembre 2018 sur un avant-projet de décret de la Communauté flamande portant approbation de la Convention du Conseil de l’Europe pour la prévention du terrorisme, faite à Varsovie le 16 mai 2005, *Doc. Parl.*, Parl. fl., 2018-2019, n° 1796/1, p. 17-18). La compétence du gouvernement fédéral va donc au-delà de la simple protection des infrastructures critiques contre les attaques terroristes. Il s’agit d’une compétence générale de protection préventive.

La nouvelle directive CER réaffirme cette “approche tous risques”, sans établir de priorités entre les types de menaces, étant donné que le paysage des menaces est dynamique. Il est clair que les deux directives reposent sur la même “approche tous risques”, bien que la directive ICE actuelle donnât la priorité à la lutte contre les menaces terroristes. Par conséquent, la transposition de la directive CER relève également de la compétence

bovengenoemde algemene preventieve beschermingsbevoegdheid van de federale overheid.

De Raad van State bevestigde bovenstaand standpunt opnieuw in hun advies nr. 76.573/2/V van 12 augustus 2024 over een voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten.

De in dit ontwerp te vinden evolutie van kritieke infrastructuur naar kritieke entiteit wijzigt niets aan de grondslag van de wetgeving. Deze blijft zich gronden in het gebied van de openbare veiligheid. Het doel van dit ontwerp is namelijk net om de bescherming en beveiliging van kritieke entiteiten te verhogen, en om deze entiteiten weerbaar te maken tegen alle mogelijke soorten risico's. Kritieke entiteiten zijn vitaal in onze samenleving, aangezien zij hieraan essentiële diensten verlenen die noodzakelijk zijn voor haar instandhouding en vooruitgang. De kritieke entiteiten moeten zich voorbereiden op de gevolgen die al deze soorten risico's kunnen hebben op hun infrastructuur door het nemen van gepaste maatregelen. Deze maatregelen worden niet genomen met het doel om de risico's zélf te mitigeren, wat een belangrijke nuance inhoudt. Zo zullen kritieke entiteiten maatregelen moeten nemen om natuurlijke risico's te mitigeren ten aanzien van hun eigen kritieke infrastructuren. Dit brengt niet met zich mee dat deze maatregelen genomen moeten worden om de klimaatverandering in het algemeen te mitigeren. De genomen maatregelen hebben steeds een duidelijke veiligheidsdimensie.

Voor wat betreft de inspecties van de weerbaarheidsmaatregelen, die uitgevoerd moeten worden door de inspectiedienst, dient fragmentatie te worden vermeden aangezien de maatregelen één geheel vormen, en als geheel beoordeeld moeten worden om efficiënt te kunnen controleren of deze maatregelen volstaan om de weerbaarheid van de kritieke entiteiten te waarborgen. De inspecties dienen aldus afgestemd en gecoördineerd te worden in één inspectiedienst. Doch is het op grond van de delegatie die gegeven wordt aan de Koning mogelijk dat sectorale overheden, indien zij dit opportuun en noodzakelijk achten, de gefedereerde entiteiten hierbij kunnen betrekken. De maatregelen zullen door de inspectiedienst niet ten gronde zelf worden beoordeeld, maar op basis van hun effectiviteit voor de bescherming van de kritieke entiteiten, in het kader van het reglementeren van de openbare veiligheid.

Artikel 26 van de CER-Richtlijn bepaalt dat de Richtlijn uiterlijk op 17 oktober 2024 omgezet moet zijn. Bijgevolg treedt deze wetgeving best van kracht voor of ten laatste op deze datum, zodat het proces van identificatie en aanduiding van start kan gaan. Zo niet, stelt de Belgische Staat zich bloot aan inbreukprocedures, ofwel omwille

générale de protection préventive susmentionnée du gouvernement fédéral.

Le Conseil d'État a réaffirmé cette position dans son avis n° 76.573/2/V du 12 août 2024 sur un avant-projet de loi relative à la résilience des entités critiques.

L'évolution que l'on trouve dans ce projet de la notion d'infrastructure critique vers celle d'entité critique ne modifie pas la base de la législation. Celle-ci reste ancrée dans le domaine de la sécurité publique. En effet, l'objectif de ce projet est précisément d'accroître la protection et la sécurité des entités critiques et de les rendre résilientes à toutes les sortes de risques possibles. Les entités critiques sont vitales pour notre société, car elles lui fournissent des services essentiels à son maintien et à son progrès. Les entités critiques doivent se préparer aux conséquences que tous ces types de risques peuvent avoir sur leurs infrastructures, en adoptant des mesures adéquates. Ces mesures ne sont pas prises dans le but d'atténuer les risques proprement dits, ce qui constitue une nuance importante. Les entités critiques devront donc adopter des mesures pour atténuer les risques naturels en ce qui concerne leurs propres infrastructures critiques. Cela ne signifie pas que ces mesures doivent être prises pour atténuer le changement climatique en général. Les mesures prises ont toujours une dimension sécuritaire évidente.

En ce qui concerne les inspections des mesures de résilience, qui doivent être effectuées par le service d'inspection, il s'agit d'éviter toute fragmentation, car les mesures forment un tout et doivent être évaluées dans leur ensemble afin de pouvoir vérifier efficacement si elles sont suffisantes pour garantir la résilience des entités critiques. Les inspections devraient donc être alignées et coordonnées au sein d'un seul service d'inspection. Toutefois, en vertu de la délégation donnée au Roi, il est possible pour les autorités sectorielles, si elles le jugent opportun et nécessaire, d'y associer les entités fédérées. Ces mesures seront évaluées par le service d'inspection non pas sur le fond, mais sur la base de leur efficacité en termes de protection des entités critiques, dans le cadre de la réglementation de la sécurité publique.

L'article 26 de la directive CER précise que la directive doit être transposée au plus tard le 17 octobre 2024. Il est donc préférable que cette législation entre en vigueur avant ou au plus tard à cette date, afin que le processus d'identification et de désignation puisse être entamé. À défaut, l'État belge s'expose à des procédures d'infraction,

van laattijdige omzetting, ofwel wegens slechte uitvoering van het Europese recht, wat dient te worden vermeden.

De sectorale overheden zullen voor hun bevoegde sectoren de verplichtingen uit deze wet moeten implementeren. Bijgevolg is het waarschijnlijk dat er op dat niveau een budgettaire impact bestaat. Dit ontwerp voorziet tevens voor verschillende bepalingen, zoals onder andere voor de inspecties en audits, een delegatie aan de Koning. Deze sectorale Koninklijke Besluiten kunnen een budgettaire impact met zich meebrengen, aangezien er bijvoorbeeld mogelijks nieuwe inspectiediensten moeten worden opgericht. De sectorale overheid is het best geplaatst om de budgettaire impact voor haar sector in te schatten.

TOELICHTING BIJ DE ARTIKELEN

HOOFDSTUK 1

Algemene bepalingen

Artikel 1

Overeenkomstig artikel 83 van de Grondwet wordt in artikel 1 van dit wetsontwerp bepaald dat het een aangelegenheid beoogt te regelen dat valt onder artikel 74 van de Grondwet.

Art. 2

Artikel 2 van het ontwerp omschrijft het voorwerp van de wet en geeft aldus uitvoering aan de verplichting van artikel 26, paragraaf 2, van de richtlijn om naar deze laatste te verwijzen bij de publicatie van de aangenomen bepalingen door een lidstaat om zich aan deze te conformeren.

HOOFDSTUK 2

Definities

Art. 3

Dit artikel bevat de definities die in het ontwerp van wet zijn gebruikt en zorgt daardoor voor de omzetting van artikel 2 van de CER-Richtlijn.

1°: deze definitie behoeft geen opmerkingen.

2° sectorale overheid: deze definitie bepaalt welke overheid voor een bepaalde sector bevoegd is.

soit pour transposition tardive, soit pour mauvaise application du droit européen, ce qu'il s'agit d'éviter.

Les autorités sectorielles doivent se conformer aux obligations découlant de la présente loi pour leurs secteurs de compétence. Par conséquent, il est probable qu'il y ait un impact budgétaire à ce niveau. En effet, ce projet prévoit une délégation au Roi pour plusieurs dispositions, telles que les inspections et les audits, entre autres. Ces arrêtés royaux sectoriels peuvent avoir un impact budgétaire, car de nouveaux services d'inspection peuvent devoir être créés, par exemple. L'autorité sectorielle est la mieux placée pour évaluer l'impact budgétaire pour son secteur.

COMMENTAIRE DES ARTICLES

CHAPITRE 1ER

Dispositions générales

Article 1er

Conformément à l'article 83 de la Constitution, l'article 1er du présent projet précise qu'il entend régler une matière visée par l'article 74 de la Constitution.

Art. 2

L'article 2 du projet définit l'objet de la loi et exécute ainsi l'obligation imposée par l'article 26, paragraphe 2, de la directive de mentionner la référence à cette dernière lors de la publication des dispositions adoptées par un État membre en vue de se conformer à celle-ci.

CHAPITRE 2

Définitions

Art. 3

Cet article contient les définitions utilisées dans le projet de loi et assure ce faisant la transposition de l'article 2 de la directive CER.

1°: cette définition n'appelle pas de remarque.

2° autorité sectorielle: cette définition détermine l'autorité compétente pour un secteur déterminé.

De sectorale overheden die, voor hun respectievelijke sector, belast zijn met de uitvoering en het toezicht op de uitvoering van de bepalingen van de wet, worden aangewezen door de wet of door de Koning bij in Ministerraad overleg besluit. Dit laat toe om nieuwe sectorale overheden op te richten, met name bestaande uit vertegenwoordigers van de federale en gefedereerde entiteiten, op basis van artikel 92*ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

Zo werd reeds het "Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater" opgericht (koninklijk besluit van 31 juli 2020 houdende de oprichting en organisatie van het Nationaal comité voor de beveiliging van de levering en distributie van drinkwater, *Belgisch Staatsblad* 20 augustus 2020), dat dienstdoet als sectorale overheid in de sector drinkwater en werd samengesteld uit vertegenwoordigers van de Federale Staat, het Vlaams Gewest, het Brussels Hoofdstedelijk Gewest en het Waals Gewest.

Punten 3° tot 9° beschrijven de verschillende basistermen die gebruikt worden in het wetsontwerp betreffende de weerbaarheid van kritieke entiteiten, die hun oorsprong vinden in de CER-Richtlijn.

Punt 3° beschrijft het begrip kritieke entiteit. Dit is de definitie die in de Richtlijn staat. Het betreft een zeer algemene definitie, aangezien een entiteit, uit de bijlage, steeds de identificatieprocedure dient te doorlopen alvorens geïdentificeerd en aangeduid te kunnen worden als kritieke entiteit. Tijdens deze identificatieprocedure worden criteria verduidelijkt op basis waarvan de entiteit als kritiek kan worden beschouwd.

4°: weerbaarheid: de CER-Richtlijn introduceerde deze term. De definitie komt uit de Richtlijn. In tegenstelling tot de KI-wet, waar de focus ligt op fysieke beveiliging en bescherming, breidt de Richtlijn deze focus uit door het gebruik van deze term. "Weerbaarheid" betekent namelijk veel meer dan enkel de fysieke beveiliging en bescherming, het houdt ook in dat entiteiten weerstand kunnen bieden aan en het kunnen mitigeren en absorberen, verwerken en herstellen van incidenten, in het kader van de bescherming van de nationale veiligheid.

Punt 5° komt uit de CER-Richtlijn en behoeft geen specifieke opmerkingen.

Punt 6° beschrijft de term kritieke infrastructuur. Dit is de definitie die in de Richtlijn staat. Deze term dient, in combinatie met punt 3°, begrepen te worden als onderdeel van de kritieke entiteit. Het onderscheid tussen deze twee termen is belangrijk om voor ogen te houden bij het opstellen en implementeren van de weerbaarheidsmaatregelen. Beide termen zijn namelijk niet los

Les autorités sectorielles qui sont chargées, pour leur secteur respectif, de la mise en œuvre et du contrôle de l'exécution des dispositions légales, sont désignées par la loi ou par le Roi par arrêté délibéré en Conseil des ministres. Cela permet la création de nouvelles autorités sectorielles, composées notamment de représentants des entités fédérales et fédérées, sur la base de l'article 92*ter* de la loi spéciale du 8 août 1980 de réformes institutionnelles.

C'est ainsi qu'a déjà été créé le "Comité national de la sécurité pour la fourniture et la distribution d'eau potable" (arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable, *Moniteur belge* 20 août 2020), qui fait office d'autorité sectorielle dans le secteur de l'eau potable et est composé de représentants de l'État fédéral, de la Région flamande, de la Région de Bruxelles-Capitale et de la Région wallonne.

Les points 3° à 9° décrivent les différents termes de base qui sont utilisés dans le projet de loi sur la résilience des entités critiques, qui trouve son origine dans la directive CER.

Le point 3° décrit la notion d'entité critique. Il s'agit de la définition qui figure dans la directive. Il s'agit d'une définition très générale, dans la mesure où une entité, de l'annexe, doit toujours parcourir la procédure d'identification avant de pouvoir être identifiée et désignée comme entité critique. Durant cette procédure, les critères sur la base desquels l'entité peut être considérée comme critique sont précisés.

4°: résilience: la directive CER a introduit ce terme. La définition découle de cette directive. Contrairement à la loi IC, qui met l'accent sur la sécurité physique et la protection, la directive élargit le champ par l'utilisation de ce terme. En effet, la "résilience" va bien au-delà de la sécurité physique et de la protection, car elle implique également que les entités puissent faire face aux incidents, les atténuer et les absorber, les traiter et s'en rétablir, dans le cadre de la protection de la sécurité nationale.

Le point 5° est issu de la directive CER et n'appelle pas de commentaire particulier.

Le point 6° définit la notion d'infrastructure critique. Il s'agit de la définition qui figure dans la directive. En combinaison avec le 3°, ce terme doit être compris comme faisant partie de l'entité critique. Il est important de garder à l'esprit la distinction entre ces deux termes lors de l'élaboration et de la mise en œuvre des mesures de résilience. Ces deux termes sont en effet

te lezen van elkaar. Het is de kritieke entiteit die in de eerste plaats geïdentificeerd en aangeduid zal worden. Als logische aanvulling op de CER-Richtlijn, wordt er in dit wetsontwerp daarnaast ook de identificatie opgelegd van de kritieke infrastructuur van een kritieke entiteit. De kritieke entiteit zelf heeft namelijk steeds fysieke infrastructuur nodig die noodzakelijk is voor de verlening van zijn essentiële dienst, en deze infrastructuur moet zich bevinden op het Belgische grondgebied. Het kan voorkomen dat een kritieke entiteit op verschillende en andere locaties in België kritieke infrastructuur bezit, dan waar zijn hoofdzetel gevestigd is. Het volstaat niet om enkel de hoofdzetel fysiek te beveiligen als de essentiële dienstverlening hiernaast afhankelijk is van infrastructuur op andere locaties in het land. Het is ook mogelijk dat een kritieke entiteit naast kritieke infrastructuur, ook niet-kritieke infrastructuur bezit. Dankzij het gebruik van beide termen kunnen deze belangrijke nuances, dewelke ontbreken op Europees niveau, wel gelegd worden op nationaal niveau.

Punten 8° tot 10°: bij deze concepten zijn geen specifieke opmerkingen nodig.

Voor de definitie van een overheidsinstantie verduidelijkt artikel 2.10 van de CER-Richtlijn dat het begrip overeenkomstig het nationale recht als zodanig erkend moet zijn, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom werd er gekozen te verwijzen naar bestaande begrippen in het Belgisch recht die de betrokken entiteiten omvatten, zodat er niet te veel verschillende begrippen zouden worden toegepast.

In dit geval verwijst de definitie naar het begrip “administratieve overheid” als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, waaraan criteria zijn toegevoegd: zij mag niet van industriële of commerciële aard zijn, niet hoofdzakelijk een activiteit uitvoeren die tot een van de andere sectoren of deelsectoren opgenomen in de bijlage bij dit wetsontwerp behoort en geen privaatrechtelijke rechtspersoon zijn.

Deze keuze wordt verklaard door het feit dat de meeste criteria in de definitie van de CER-Richtlijn terug te vinden zijn in de criteria die het begrip “administratieve overheid” als bedoeld in de gecoördineerde wetten op de Raad van State afbakenen. Daarbij wordt dezelfde definitie gebruikt in de wet van 26 april 2024 tot vaststelling van een kader voor cyberbeveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid.

De CER-Richtlijn verduidelijkt in de bijlage dat de sector overheid enkel overheidsinstanties van centrale

indissociables. C’est l’entité critique qui sera identifiée et désignée en premier lieu. En complément logique de la directive CER, le présent projet de loi impose également l’identification de l’infrastructure critique d’une entité critique. L’entité critique a en effet toujours besoin de l’infrastructure physique nécessaire à la fourniture de ses services essentiels et cette infrastructure doit se situer sur le territoire belge. Il se peut qu’une entité critique possède des infrastructures critiques dans plusieurs endroits en Belgique et dans des lieux autres que le siège central. Il ne suffit pas de sécuriser physiquement le siège central si la fourniture de services essentiels dépend d’infrastructures situées dans d’autres endroits du pays. Il se peut également qu’une entité critique possède, outre une infrastructure critique, une infrastructure non-critique. Grâce à l’utilisation des deux termes, ces nuances importantes, qui font défaut au niveau européen, peuvent être mises en exergue au niveau national.

Les points 8° à 10°: ces concepts n’appellent aucune remarque spécifique.

Pour la définition d’une entité de l’administration publique, l’article 2.10 de la directive CER précise que la notion doit être reconnue comme telle conformément au droit national, à l’exclusion de la justice, des parlements et des banques centrales. Ainsi, il a été choisi de faire référence à des notions existantes en droit belge qui couvrent les entités concernées afin de ne pas multiplier l’application de notions différentes.

En l’occurrence, la définition reprend la notion d’autorité administrative visée à l’article 14, § 1er, alinéa 1er, des lois coordonnées du 12 janvier 1973 sur le Conseil d’État, à laquelle sont rajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l’un des autres secteurs ou sous-secteurs repris dans les annexes du présent projet de loi et de ne pas être une personne morale de droit privé.

Ce choix s’explique étant donné le fait que la plupart des critères repris dans la définition de la directive se retrouvent dans les critères qui délimitent la notion d’autorité administrative au sens des lois coordonnées sur le Conseil d’État. Ainsi, la même définition est utilisée dans la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique.

La directive CER précise dans son annexe que le secteur des administrations publiques couvre uniquement

overheden betreft, zoals gedefinieerd door de lidstaat overeenkomstig het nationale recht. Het onderscheid dat gemaakt wordt in de bijlage van de NIS 2-Richtlijn tussen overheidsinstanties van centrale overheden, overheidsinstanties op regionaal niveau en overheidsinstanties op lokaal niveau, moet mee in rekening gebracht worden bij de beoordeling van het toepassingsgebied van de CER-Richtlijn. Gelet op de onderlinge afhankelijkheid tussen de CER-Richtlijn en de NIS 2 Richtlijn, kan hieruit afgeleid worden dat de Europese wetgever niet beoogt heeft de overheidsinstanties op regionaal niveau mee op te nemen in het toepassingsgebied van de CER-Richtlijn. Bijgevolg vallen overheidsinstanties die onder de bevoegdheid van deelstaten ressorteren aldus niet onder het toepassingsgebied van de CER-Richtlijn.

HOOFDSTUK 3

Toepassingsgebied

Art. 4

Dit artikel verklaart de wet van toepassing op de exclusieve economische zone (EEZ).

In principe gelden de Belgische wetten enkel op het Belgisch grondgebied, maar artikel 37 van de wet van 22 april 1999 betreffende de exclusieve economische zone van België (EEZ-wet) bepaalt dat België bezit over uitsluitende rechtsmacht over kunstmatige eilanden, installaties en inrichtingen, met inbegrip van de wetten en voorschriften inzake douane, belastingen, Volksgezondheid, veiligheid en immigratie. Daarnaast bepaalt artikel 38 van de EEZ-wet dat artikel 7 van de wet van 13 juni 1969 inzake de exploratie en de exploitatie van niet-levende rijkdommen van de territoriale zee en het continentaal plat eveneens van toepassing is op kunstmatige eilanden, installaties en inrichtingen in de EEZ die voor andere doeleinden worden gebruikt dan de exploitatie van minerale en andere niet-levende rijkdommen. Hieruit volgt dat kunstmatige eilanden, installaties of andere inrichtingen onderworpen zijn aan het Belgisch recht. Ter bevordering van de rechtszekerheid bepaalt dit artikel expliciet dat de wet van toepassing is op de EEZ.

Het is mogelijk dat er entiteiten gelegen zijn in de EEZ die voldoen aan de voorwaarden om aangeduid te worden als kritieke entiteit. Zij moeten op dezelfde wijze beschermd worden als de kritieke entiteiten die gelegen zijn op het Belgisch grondgebied, gelet op de impact die een verstoring van de levering van essentiële diensten kan hebben op België.

les entités publiques des gouvernements centraux, telles que définies par l'État membre conformément au droit national. La distinction faite dans l'annexe de la directive NIS 2 entre les autorités publiques des gouvernements centraux, les autorités publiques au niveau régional et les autorités publiques au niveau local devrait être prise en compte lors de l'évaluation du champ d'application de la directive CER. Compte tenu de l'interdépendance entre la directive CER et la directive NIS 2, on peut déduire que le législateur européen n'a pas eu l'intention d'inclure les autorités publiques au niveau régional dans le champ d'application de la directive CER. Par conséquent, les gouvernements publics relevant de la compétence des régions ne sont donc pas inclus dans le champ d'application de la directive CER.

CHAPITRE 3

Champ d'application

Art. 4

Cet article déclare le droit applicable à la zone économique exclusive (ZEE).

En principe, les lois belges ne s'appliquent que sur le territoire belge, mais l'article 37 de la loi du 22 avril 1999 relative à la zone économique exclusive de la Belgique (loi ZEE) stipule que la Belgique possède une compétence exclusive sur les îles artificielles, les installations et les établissements, y compris les lois et règlements en matière de douane, de fiscalité, de santé publique, de sécurité et d'immigration. En outre, l'article 38 de la loi ZEE prévoit que l'article 7 de la loi du 13 juin 1969 relative à l'exploration et à l'exploitation des ressources non biologiques de la mer territoriale et du plateau continental s'applique également aux îles artificielles, installations et établissements de la ZEE utilisés à des fins autres que l'exploitation des ressources minérales et autres ressources non biologiques. Il s'ensuit que les îles artificielles, installations ou autres établissements sont soumis au droit belge. Dans un souci de sécurité juridique, cet article précise explicitement que la loi s'applique à la ZEE.

Il peut y avoir des entités situées dans la ZEE qui remplissent les conditions pour être désignées comme entités critiques. Elles devraient être protégées de la même manière que les entités critiques situées sur le territoire belge, étant donné l'impact qu'une interruption de la fourniture de services essentiels peut avoir sur la Belgique.

Art. 5

Dit artikel bepaalt het toepassingsgebied van dit ontwerp, namelijk de sectoren opgesomd in de bijlage. Dit artikel, in combinatie met de bijlage bij het ontwerp, zet aldus de bijlage van de Richtlijn om.

Wat betreft de energiesector, bepaalt de vijfde overweging van de Richtlijn dat de “elektriciteitsproductie ook de transmissieonderdelen van kerncentrales kan omvatten, maar niet de specifiek nucleaire elementen die vallen onder verdragen en het Unierecht, met inbegrip van relevante rechtshandelingen van de Unie betreffende kernenergie”. Het is deze uitsluiting die het tweede lid van deze paragraaf voorziet, verwijzend naar de nucleaire installaties bedoeld in de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle. Enkel de elementen van een nucleaire installatie bestemd voor de industriële productie die dienen voor de transmissie van de elektriciteit kunnen dus vallen binnen het toepassingsgebied van deze wet. Dit werd op dezelfde manier geregeld in de KI-wet.

Art. 6

Paragraaf 1 bepaalt dat de desbetreffende bepalingen uit dit ontwerp niet van toepassing zijn aangezien bepalingen van sectorspecifieke rechtshandelingen van de Unie aan kritieke entiteiten uit de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuren, reeds voorschrijven om maatregelen te nemen die hun weerbaarheid vergroten, teneinde dubbel werk en onnodige last te voorkomen, en harmonisatie tussen de lidstaten te waarborgen. In dat geval gelden de relevante rechtsbepalingen van dergelijke rechtshandelingen. Deze aanpak zorgt voor consistentie tussen de CER-Richtlijn, de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad en de Verordening (EU) 2022/2554 van het Europees Parlement en de Raad betreffende digitale operationele weerbaarheid van de financiële sector. De Koning kan evenwel bepalen dat er in deze sectoren tot een hoger weerbaarheidsniveau moet gekomen worden, wanneer blijkt dat de sectorspecifieke regelgeving niet hetzelfde weerbaarheidsniveau kan garanderen.

Paragraaf 2 bevat een algemene equivalentiebepaling, dewelke bepaalt dat wanneer bepalingen van sector en deel-sectorspecifieke wetgeving vereisen dat kritieke entiteiten maatregelen nemen om hun weerbaarheid te vergroten, en als gelijkwaardig geacht worden door de Koning, deze verplichtingen uit hoofde van hoofdstuk 4,

Art. 5

Cet article définit le champ d’application du présent projet, à savoir les secteurs énumérés en annexe. Combiné à l’annexe du projet, cet article transpose donc l’annexe de la directive.

En ce qui concerne le secteur de l’énergie, le cinquième considérant de la directive énonce que “la production de l’électricité peut englober les éléments des centrales nucléaires servant au transport de l’électricité, tout en excluant les éléments strictement nucléaires, qui relèvent du droit de l’Union, y compris les actes juridiques pertinents de l’Union concernant l’énergie nucléaire”. C’est cette exclusion que prévoit le deuxième alinéa de ce paragraphe, faisant référence aux installations nucléaires visées par la loi du 15 avril 1994 relative à la protection de la population et de l’environnement contre les dangers résultant des rayonnements ionisants et relative à l’Agence fédérale de Contrôle nucléaire. Seuls les éléments d’une installation nucléaire destinée à la production industrielle d’électricité qui servent au transport de l’électricité peuvent donc relever du champ d’application de la présente loi. Ce point était réglementé de la même manière dans la loi IC.

Art. 6

Le paragraphe 1er prévoit que les dispositions pertinentes du présent projet ne s’appliquent pas, parce que des dispositions d’actes juridiques sectoriels de l’Union imposent déjà aux entités critiques des secteurs de la banque, d’infrastructure des marchés financiers et d’infrastructure digitale de prendre des mesures pour accroître leur résilience, afin d’éviter les doubles emplois et les charges inutiles, ainsi que d’assurer l’harmonisation entre les États membres. Dans ce cas, les dispositions pertinentes de ces actes juridiques s’appliqueront. Cette approche garantit la cohérence entre la directive CER, la directive (UE) 2022/2555 du Parlement européen et du Conseil et le règlement (UE) 2022/2554 du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier. Toutefois, le Roi peut déterminer qu’un niveau de résilience plus élevé doit être atteint dans ces secteurs s’il apparaît que les réglementations sectorielles ne peuvent pas garantir le même niveau de résilience.

Le paragraphe 2 contient une disposition générale d’équivalence, qui prévoit que lorsque des dispositions de la législation sectorielle et sous-sectorielle exigent des entités critiques qu’elles prennent des mesures pour renforcer leur résilience, et qu’elles sont jugées équivalentes par le Roi, les obligations prévues au chapitre 4,

afdeling 2, hoofdstuk 5 en hoofdstuk 7 uit dit ontwerp niet van toepassing zijn op die entiteiten.

Art. 7

De CER-Richtlijn bepaalt dat de Richtlijn geen afbreuk doet aan de bevoegdheden van de lidstaten en hun autoriteiten op het gebied van bestuurlijke autonomie, en evenmin aan hun verantwoordelijkheid om de nationale veiligheid en defensie te waarborgen of hun bevoegdheid om andere essentiële staatsfuncties te beschermen, met name op het gebied van openbare veiligheid, territoriale integriteit en het handhaven van de openbare orde. Bijgevolg worden overheidsinstanties volledig uitgesloten van het toepassingsgebied van de wet indien de activiteiten hoofdzakelijk worden uitgevoerd op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten. Wanneer de activiteiten van de overheidsinstantie slechts zijdelings verband houdt met die gebieden, moeten zij evenwel vallen onder het toepassingsgebied van de wet.

Het kan voorkomen dat kritieke entiteiten uit andere sectoren hoofdzakelijk activiteiten verrichten op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten, of uitsluitend diensten verlenen aan overheidsinstanties die hoofdzakelijk activiteiten verrichten op die gebieden. Voor deze entiteiten moet besloten worden dat de verplichtingen uit de wet voor de kritieke entiteiten die zijn vastgelegd in de wet in hoofdstuk 4, afdeling 2, en hoofdstukken 5 en 7, niet van toepassing zijn op deze kritieke entiteiten. Dit is het voorwerp van paragraaf 2.

HOOFDSTUK 4

Afdeling 1

Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructuren

Art. 8

Artikel 8 van dit ontwerp zet artikel 5 van de CER-Richtlijn om en betreft de risico gebaseerde aanpak die de identificatieprocedure uit dit ontwerp onderbouwt.

De sectorale overheid stelt, als startpunt in de identificatieprocedure, een lijst op van essentiële diensten van de in de bijlage genoemde sectoren en deelsectoren die onder haar bevoegdheid valt. De sectorale overheid

à la section 2, au chapitre 5 et au chapitre 7 du présent projet ne s'appliquent pas à ces entités.

Art. 7

La directive CER précise qu'elle n'affecte pas les compétences des États membres et de leurs autorités en termes d'autonomie administrative, ni leur responsabilité en matière de sauvegarde de la sécurité et de la défense nationales, ni leur compétence en matière de protection d'autres fonctions essentielles de l'État, notamment la sécurité publique, l'intégrité territoriale et le maintien de l'ordre public. En conséquence, les organismes publics sont totalement exclus du champ d'application de la loi si les activités sont menées principalement dans le domaine de la sécurité nationale, de la sûreté publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales. Toutefois, si les activités de l'organisme public ne sont qu'indirectement liées à ces domaines, elles doivent entrer dans le champ d'application de la loi.

Il peut arriver que des entités critiques d'autres secteurs exercent des activités principalement dans les domaines de la sécurité nationale, de la sûreté publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales, ou fournissent exclusivement des services aux autorités publiques qui exercent des activités principalement dans ces domaines. Pour ces entités, il convient de décider que les obligations prévues par la loi pour les entités critiques au chapitre 4, section 2, et aux chapitres 5 et 7 ne s'appliquent pas à ces entités critiques. C'est l'objet du paragraphe 2.

CHAPITRE 4

Section 1re

Identification et désignation des entités critiques et des infrastructures critiques

Art. 8

L'article 8 du présent projet transpose l'article 5 de la directive CER et concerne l'approche basée sur les risques qui sous-tend la procédure d'identification visée par le projet.

Comme point de départ de la procédure d'identification, l'autorité sectorielle établit une liste des services essentiels des secteurs et sous-secteurs visés en annexe qui relèvent de sa compétence. L'autorité sectorielle base

baseert deze lijst op de lijst van essentiële diensten die werd opgesteld door de Commissie in de gedelegeerde Verordening (EU) van 27 juli 2023, op grond van artikel 5, paragraaf 1 van de CER-Richtlijn. De sectorale overheid kan indien nodig aan deze lijst nog andere essentiële diensten, die zij geïdentificeerd hebben in hun welbepaalde sector of deelsector, toevoegen.

Paragraaf 2 houdt de verplichting in voor de sectorale overheid om een sectorale risicobeoordeling uit te voeren, alvorens kritieke entiteiten te kunnen identificeren. De verantwoordelijkheid hiervoor valt op de sectorale overheden, aangezien zij beschikken over de nodige expertise in hun welbepaalde sectoren of deelsectoren. Deze risicobeoordeling moet voor de eerste maal uitgevoerd worden uiterlijk op 17 januari 2026, en vervolgens telkens wanneer nodig en ten minste om de vier jaar. Deze risicobeoordeling zal hierna tijdens de identificatieprocedure gebruikt kunnen worden. Tijdens de identificatieprocedure zal men zowel rekening moeten houden met de risico's waaraan een entiteit kan blootgesteld worden, als de impact dat een verstoring van de werking op de essentiële dienstverlening met zich mee kan brengen.

Deze risicobeoordeling wordt tevens nadien gedeeld met de geïdentificeerde kritieke entiteiten. De sectorale overheden staan de kritieke entiteiten bij aan de hand van informatie-uitwisseling bij het nemen van de weerbaarheidsmaatregelen zoals voorzien in artikel 18. De financiële verantwoordelijkheid voor het nemen van deze maatregelen blijft evenwel steeds volledig bij de kritieke entiteit liggen.

De derde paragraaf omschrijft de inhoud van deze risicobeoordeling, door o.a. te vermelden met welke risico's men rekening moet houden tijdens het uitvoeren ervan. Bij het uitvoeren van de risicobeoordeling moet tevens rekening gehouden worden met andere algemene of sectorspecifieke risicobeoordelingen die krachtens andere rechtshandelingen van de Unie zijn verricht. Hieronder valt bijvoorbeeld de *Belgian National Risk Assessment* (BNRA), dewelke een algemene risicobeoordeling inhoudt over alle mogelijke risico's waaraan België kan blootgesteld worden (Art. 6, a), van Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad). De BNRA wordt gecoördineerd door het NCCN, met behulp van tal van experten, en de relevante informatie hiervan wordt gedeeld aan de bevoegde sectorale overheden zodat dit mee opgenomen kan worden in de sectorale risicobeoordeling. Hiernaast bestaat er in sommige sectoren nog sectorspecifieke wetgeving, op basis waarvan reeds risicobeoordelingen moet worden uitgevoerd (Verordening (EU) 2019/947 van het Europees Parlement en de Raad, Verordening (EU) 2017/1938 van

cette liste sur la liste des services essentiels qui a été établie par la Commission dans le règlement délégué (UE) du 27 juin 2023, en vertu de l'article 5, paragraphe 1 la directive CER. Si nécessaire, l'autorité sectorielle peut ajouter à cette liste d'autres services essentiels qu'elle a identifiés dans son secteur ou sous-secteur déterminé.

Le paragraphe 2 oblige l'autorité sectorielle à mener une évaluation des risques sectoriels avant de pouvoir identifier les entités critiques. La responsabilité à cet égard incombe aux autorités sectorielles étant donné qu'elles disposent de l'expertise nécessaire dans leurs secteurs ou sous-secteurs déterminés. Cette évaluation des risques doit être effectuée pour la première fois le 17 janvier 2026 au plus tard, ensuite chaque fois que cela s'avère nécessaire et au moins tous les quatre ans. Elle pourra servir ensuite durant la procédure d'identification. Au cours du processus d'identification, il sera nécessaire d'examiner à la fois les risques auxquels une entité peut être exposée et l'impact qu'une interruption de fonctionnement peut avoir sur les services essentiels.

Cette évaluation des risques est également communiquée par la suite aux entités critiques identifiées. Les autorités sectorielles fournissent leur aide aux entités critiques en partageant des informations lors de la prise des mesures de résilience prévues à l'article 18. Toutefois, la responsabilité financière de ces mesures incombe toujours entièrement à l'entité critique.

Le troisième paragraphe définit le contenu de cette évaluation des risques, en mentionnant notamment les risques à prendre en compte au moment de sa réalisation. Durant l'évaluation des risques, il y a également lieu de tenir compte d'évaluations des risques générales ou sectorielles qui ont été menées en vertu d'autres actes juridiques de l'Union. C'est notamment le cas du *Belgian National Risk Assessment* (BNRA), qui porte sur l'évaluation générale de tous les risques potentiels auxquels la Belgique peut être confrontée (Art. 6, a), de la décision n° 1313/2013/UE du Parlement européen et du Conseil). Le BNRA est coordonné par le NCCN, avec l'aide de nombreux d'experts, et les informations pertinentes sont partagées avec les autorités sectorielles compétentes pour pouvoir être intégrées dans l'évaluation sectorielle des risques. Il existe en outre, dans certains secteurs, des législations sectorielles spécifiques, sur la base desquelles des évaluations des risques doivent déjà être effectuées (règlement (UE) 2019/947 du Parlement européen et du Conseil, règlement (UE) 2017/1938 du Parlement européen et du Conseil, directive 2012/18/

het Europees Parlement en de Raad, Richtlijn 2012/18/EU van het Europees Parlement en de Raad, en Richtlijn 2007/60/EG van het Europees Parlement en de Raad).

Art. 9

Het OCAD voert een dreigingsanalyse uit voor de (deel)sectoren vermeld in bijlage. Deze dreigingsanalyse vond zijn oorsprong in de KI-wet maar past in het kader van de alle risico's benadering uit de Richtlijn. In de KI-wet werd deze dreigingsanalyse pas aangevraagd na de identificatie van de kritieke infrastructuur. Deze stap werd in dit ontwerp vervroegd, waardoor de dreigingsanalyse een analyse van de sector of deelsector zal betreffen in plaats van de kritieke entiteiten zelf. Op deze manier kunnen de sectorale overheden de informatie uit deze dreigingsanalyse mee kunnen opnemen in hun risicobeoordeling zoals bedoeld in artikel 8. De dreigingsanalyse zal daarna ook gedeeld worden met de kritieke entiteiten, zodat ook zij de relevante informatie hieruit kunnen opnemen in hun eigen risicobeoordeling.

Alle dreigingsanalyses zijn vier jaar geldig. Dit betekent dat analyses die voor de inwerkingtreding van deze wet uitgevoerd werden, en niet ouder zijn dan deze vier jaar, nog steeds geldig zijn in het kader van dit ontwerp, tot dat deze termijn van vier jaar afloopt.

Alle dreigingsanalyses moeten worden vernieuwd wanneer dat nodig is, hetgeen wordt beoordeeld in overeenstemming met het OCAD, bijvoorbeeld wanneer een nieuwe gebeurtenis de analyse wijzigt, hetzij met betrekking tot een nieuw type dreiging of met betrekking tot inlichtingen die de waarschijnlijkheid of de impact van een type dreiging wijzigen.

Paragraaf 2 omschrijft de dreigingsanalyse in de zin van hoofdstuk 4 van dit ontwerp.

De aard van de analyse wordt gepreciseerd: het gaat om een strategische gemeenschappelijke evaluatie in de zin van artikel 8, eerste lid, 1°, van de wet van 10 juli 2006 betreffende de dreigingsanalyse, zij het met een verschil in de draagwijdte van de dreigingen waarmee rekening wordt gehouden. De dreigingsanalyse, die door artikel 3 van de wet van 10 juli 2006 betreffende de dreigingsanalyse momenteel beperkt is tot dreigingen die ontstaan uit terrorisme en extremisme, werd reeds in de KI-wet voor de bescherming van kritieke infrastructuren uitgebreid tot elk type van dreiging die onder de bevoegdheid van de ondersteunende diensten valt zoals bedoeld in het artikel 2, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, wanneer die door het OCAD pertinent worden geacht ten aanzien van de

UE du Parlement européen et du Conseil, et directive 2007/60/CE du Parlement européen et du Conseil).

Art. 9

L'OCAM effectue une analyse des menaces pour les (sous-)secteurs énumérés en annexe. Cette analyse de la menace trouve son origine dans la loi IC, mais s'inscrit dans le cadre de l'approche tous risques de la directive CER. Dans la loi IC, cette analyse de la menace n'était demandée qu'après l'identification des infrastructures critiques. Cette étape a été avancée dans le présent projet, ce qui aboutira à une analyse de la menace du secteur ou du sous-secteur plutôt qu'à une analyse de la menace des entités critiques. De cette manière, les autorités sectorielles puissent inclure les informations de cette analyse de la menace dans leur évaluation des risques visée à l'article 8. L'analyse de la menace sera ensuite également partagée avec les entités critiques afin qu'elles puissent elles aussi inclure les informations pertinentes dans leur propre évaluation des risques.

Toutes les analyse de la menace sont valables quatre ans. Cela signifie que les analyses effectuées avant l'entrée en vigueur de cette loi, et ne datant pas de plus de quatre ans, restent valables en vertu de ce projet jusqu'à l'expiration de cette période de quatre ans.

Toutes les analyses de la menace doivent être renouvelées chaque fois que nécessaire, ce qui est évalué en accord avec l'OCAM, par exemple lorsqu'un nouvel évènement modifie cette analyse, qu'il s'agisse soit d'un nouveau type de menace, soit de renseignements qui modifient la probabilité ou l'impact d'un type de menace.

Le paragraphe 2 définit l'analyse de la menace au sens du chapitre 4 du présent projet.

La nature de l'analyse est précisée: il s'agit d'une évaluation stratégique commune au sens de l'article 8, alinéa 1er, 1° de la loi du 10 juillet 2006 relative à l'analyse de la menace, avec néanmoins une différence quant à l'étendue du champ des menaces prises en considération. L'analyse de la menace, qui est actuellement limitée aux menaces liées au terrorisme et à l'extrémisme par l'article 3 de la loi du 10 juillet 2006 relative à l'analyse de la menace, a déjà été étendue dans la loi IC, pour la protection des infrastructures critiques, à tout type de menace relevant de la compétence des services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, lorsque l'OCAM le juge pertinent par rapport au secteur ou au sous-secteur. Rien de cela n'a été modifié. Ceci est justifié, d'une part, par

sector of deelsector. Hier wordt niets aan gewijzigd. Dat is enerzijds gerechtvaardigd door het feit dat terrorisme en extremisme slechts een klein deel uitmaken van de alle risico's benadering van de Richtlijn en anderzijds door de aanzienlijke weerslag die de verstoring van de werking of van de vernietiging van een kritieke entiteiten in het land zou hebben.

De analyse van de dreiging wordt hier gedefinieerd verwijzend naar de taken van de ondersteunende diensten bedoeld bij artikel 2, 2° van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

Het gaat om de volgende diensten:

"a) de inlichtingen- en veiligheidsdiensten, zoals bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, hierna de "wet houdende regeling van de inlichtingen- en veiligheidsdienst" genoemd;

b) de politiediensten zoals bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

c) de Federale Overheidsdienst Financiën, in het bijzonder de Administratie der Douane en Accijnzen;

d) de Federale Overheidsdienst Mobiliteit en Vervoer;

e) de Federale Overheidsdienst Binnenlandse Zaken, in het bijzonder de Dienst Vreemdelingenzaken;

f) de Federale Overheidsdienst Buitenlandse Zaken;

f/1) de Federale Overheidsdienst Binnenlandse Zaken, in het bijzonder het Nationaal Crisiscentrum;

f/2) de Federale Overheidsdienst Justitie, in het bijzonder het Directoraat-generaal Penitentiaire inrichtingen;

f/3) de Federale Overheidsdienst Justitie, in het bijzonder de dienst Erediensten en Vrijzinnigheid van het Directoraat-generaal Wetgeving, Fundamentele rechten en Vrijheden;

f/4) de federale overheidsdienst Financiën, in het bijzonder de algemene administratie van de Thesaurie;

g) de door de Koning op voorstel van de Nationale Veiligheidsraad aangewezen overheidsdiensten."

Wat betreft de inlichtingen- en veiligheidsdiensten, preciseert artikel 7, 1°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst dat "De Veiligheid van de Staat (…) als

le fait que le terrorisme et l'extrémisme ne constituent qu'une petite partie de l'approche tous risques de la directive CER et, d'autre part, par l'impact important que l'interruption du fonctionnement ou la destruction d'une entité critique aurait sur le pays.

L'analyse de la menace est définie en faisant référence aux tâches des services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace.

Il s'agit des services suivants:

"a) les services de renseignement et de sécurité tels que visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, ci-après dénommée la "loi organique des services de renseignement et de sécurité";

b) les services de police tels que visés dans la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

c) le Service public fédéral Finances, en particulier l'Administration des Douanes et Accises;

d) le Service public fédéral Mobilité et Transport;

e) le Service public fédéral Intérieur, en particulier l'Office des Étrangers;

f) le Service public fédéral Affaires étrangères;

f/1) le Service public fédéral Intérieur, en particulier le Centre de Crise National;

f/2) le Service public fédéral Justice, en particulier la direction générale Établissements pénitentiaires;

f/3) le Service public fédéral Justice, en particulier le Service des Cultes et de la Laïcité de la Direction générale, Législation, libertés et droits fondamentaux;

f/4) le Service public fédéral Finances, en particulier l'administration générale de la Trésorerie;

g) les services publics désignés par le Roi, sur la proposition du Conseil national de sécurité."

En ce qui concerne les services de renseignement et de sécurité, l'article 7, 1°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité précise que "La Sûreté de l'État (…) a pour mission:

opdracht heeft: 1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;" en artikel 11, § 1, 1° en 2°, dat "De Algemene Dienst Inlichting en Veiligheid, belast met de nationale veiligheid, heeft als opdracht:

1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:

a) de onschendbaarheid van het nationaal grondgebied of de bevolking,

b) de militaire defensieplannen,

c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,

d) de vervulling van de opdrachten van de strijd-krachten,

e) de veiligheid van de Belgische onderdanen in het buitenland,

f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad,

bedreigt of zou kunnen bedreigen en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;

2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen,

1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité; (…)"; et l'article 11, § 1er, 1° et 2°, que "Le Service Général du Renseignement et de la Sécurité, chargé de la sécurité nationale, a pour mission:

1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:

a) l'intégrité du territoire national ou la population,

b) les plans de défense militaires,

c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,

d) l'accomplissement des missions des Forces armées,

e) la sécurité des ressortissants belges à l'étranger,

f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité,

et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;

2° de veiller au maintien de la sécurité militaire du personnel relevant du ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents,

geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht."

De dreigingen die vallen onder de bevoegdheden van deze diensten zijn dus divers. Het vloeit overigens voort uit de opdrachten van de politiediensten, gedefinieerd door de artikelen 14 en 15 van de wet op het politieambt, om namelijk misdrijven te voorkomen, de daders ervan op te sporen of nog personen en goederen te beschermen, zijnde opdrachten die gelijk welk type van dreiging dekken. Er wordt dus tegemoetgekomen aan het doel van de CER-Richtlijn om een "alle risico's omvattende aanpak" te beogen.

Alle relevante informatie waarover het NCCN en de sectorale overheden beschikken, wordt gedeeld met het OCAD. Het betreft slechts een overdracht van gegevens die al wettelijk zijn verzameld door andere overheidsinstanties. Daarnaast gaat het bij de doorgifte vaak niet om persoonsgegevens maar over gebeurtenissen. In dit verband is het belangrijk om te benadrukken dat deze gegevens door het OCAD niet worden gebruikt om individuele beslissingen van administratieve of gerechtelijke aard te nemen, bijvoorbeeld met betrekking tot specifieke personen, maar om dreigingsanalyses uit te voeren.

Gelet op het feit dat de dreigingsanalyse in dit ontwerp plaatsvindt voor de officiële aanduiding van kritieke entiteiten, is het mogelijk dat de sectorale overheid over sectorspecifieke informatie beschikt die relevant kan zijn voor de uitvoering van de dreigingsanalyse. De communicatieplicht die rust op de sectorale overheden is beperkt tot de mededeling van gegevens die uitdrukkelijk door het OCAD worden gevraagd en die zij reeds in het kader van hun opdrachten in bezit hebben.

Dergelijke relevante informatie kan onder meer de incidentenmeldingen door kritieke entiteiten inhouden.

Art. 10

Artikel 10 bevat de omzetting van artikel 6 van de CER-Richtlijn, en omschrijft het identificatieproces voor kritieke entiteiten. Er werden enkele stappen aan het identificatieproces uit de KI-wet toegevoegd teneinde beter overeen te stemmen met de CER-Richtlijn.

systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés."

Les menaces qui relèvent des compétences de ces services sont donc variées. Il découle par ailleurs des articles 14 et 15 de la loi sur la fonction de police que la prévention des délits, la recherche des auteurs ou la protection des personnes et des biens sont des missions des services de police qui couvrent tout type de menace. L'objectif de la directive CER, qui consiste en une "approche tous risques", est dès lors atteint.

Toutes les informations pertinentes à la disposition du NCCN et des autorités sectorielles sont communiquées à l'OCAM. Il s'agit simplement d'un transfert de données déjà légalement collectées par d'autres autorités publiques. En outre, souvent, le transfert ne porte pas sur des données à caractère personnel mais sur des événements. Dans ce contexte, il est important de souligner que ces données ne sont pas utilisées par l'OCAM pour prendre des décisions individuelles de nature administrative ou judiciaire, par exemple concernant des personnes spécifiques, mais pour effectuer des évaluations de la menace.

Étant donné que l'analyse de la menace dans ce projet a lieu avant la désignation officielle des entités critiques, il est possible que l'autorité sectorielle dispose d'informations spécifiques au secteur qui pourraient être utiles pour effectuer l'analyse de la menace. L'obligation de communication incombant aux autorités sectorielles est limitée à la communication des données explicitement demandées par l'OCAM et déjà détenues par elles dans le cadre de leurs missions.

Ces informations pertinentes peuvent comprendre des rapports d'incidents émis par des entités critiques.

Art. 10

L'article 10 contient la transposition de l'article 6 de la directive CER et définit le processus d'identification des entités critiques. Par rapport aux procédures actuelles prévues par la loi IC, certaines étapes ont été ajoutées pour mieux correspondre à la directive CER.

Paragraaf 1 houdt de chronologische volgorde van de identificatieprocedure in. Er wordt verwezen naar de uitleg bij artikel 21, waarin wordt verduidelijkt dat het NCCN aangeduid wordt als bevoegde autoriteit.

Teneinde de kritieke entiteiten te identificeren, overlegt de sectorale overheid vooraf met het NCCN. Zij zal tevens de vertegenwoordigers van de betrokken sector en de potentiële kritieke entiteiten kunnen raadplegen. Een dergelijke raadpleging zal immers toelaten aan de sectorale overheid om te beschikken over een duidelijke visie op de sector en de betrokken activiteiten en zal eveneens een betere uitvoering van deze wetgeving door de entiteit moeten toelaten, die in eerste instantie zal betrokken zijn in het proces. Deze raadpleging zorgt er ook voor dat de kritieke entiteiten op de hoogte zijn van de identificatieprocedure en het feit dat zij potentieel aangeduid kunnen worden als kritieke entiteit. De entiteit kan zich dan beter voorbereiden en kan ook reeds van start gaan met de identificatie van de kritieke infrastructuren waar zij als kritieke entiteit van afhankelijk zijn.

Eveneens zal de sectorale overheid de gefedereerde entiteiten kunnen raadplegen, indien de potentiële kritieke infrastructuren onder hun bevoegdheden vallen. Het standpunt van de Raad van State in zijn advies van 9 december 2010 over de wet van 1 juli 2011 met betrekking tot de beveiliging en bescherming van kritieke infrastructuur, was dat aangezien de gefedereerde entiteiten bevoegdheden bezitten op het gebied van de betrokken sectoren uit die wet, bij uitvoering ervan een weerslag van sommige van de maatregelen voelbaar kan zijn in het beheer van de infrastructuur die tot de bevoegdheid van de gefedereerde entiteiten horen. Er werd aldus aanvaard dat zij wel betrokken kunnen worden in het proces, doch de autonomie van de federale overheid gerespecteerd wordt, aangezien een consultatie vrijwillig is en de aanname van maatregelen door de federale overheid niet kan verhinderen (RvS 9 december 2010, advies nr. 48.989/VR, p.4).

Dit ontwerp behelst de verschillende aspecten van weerbaarheid van kritieke entiteiten waarbij de bescherming en beveiliging ervan één van de elementen is die al degelijk werden uitgewerkt in de KI-wet. Wat in het verleden werd opgebouwd blijft aldus behouden en wordt geïntegreerd, samen met het verhogen van de weerbaarheid ten aanzien van alle risico's die gevat worden in de CER-Richtlijn waarvan deze CER-wet de omzetting is.

Deze identificatieprocedure gebeurt met toepassing van de hierna gedefinieerde criteria.

In de tweede paragraaf wordt beschreven hoe de identificatie verloopt van de kritieke infrastructuren onder

Le paragraphe 1er porte sur l'ordre chronologique de la procédure d'identification. Il convient de se référer à l'explication de l'article 21, qui précise que le NCCN est désigné comme l'autorité compétente.

Afin d'identifier les entités critiques, l'autorité sectorielle consulte préalablement le NCCN. Elle pourra également consulter les représentants du secteur concerné et des potentielles entités critiques. Cette consultation permettra en effet à l'autorité sectorielle de disposer d'une vision claire du secteur et des activités concernées, et devrait également améliorer la mise en œuvre de cette législation par l'entité qui sera impliquée en premier lieu dans le processus. Grâce à cette consultation, les entités critiques seront en outre au courant de la procédure d'identification et du fait qu'elles peuvent potentiellement être désignées comme entité critique. L'entité pourra ainsi mieux se préparer et entamer d'ores et déjà l'identification des infrastructures critiques dont elle dépend en tant qu'entité critique.

L'autorité sectorielle pourra aussi consulter les entités fédérées, si les infrastructures critiques potentielles relèvent de leurs compétences. Dans son avis du 9 décembre 2010 concernant la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, le point de vue du Conseil d'État était le suivant: dans la mesure où les entités fédérées disposent de compétences dans le domaine des secteurs concernés par cette loi, certaines mesures peuvent, au moment de leur mise en œuvre, avoir des répercussions sur la gestion de l'infrastructure qui relève de la compétence des entités fédérées. Il a dès lors été admis qu'elles peuvent être associées au processus, mais doivent respecter l'autonomie des autorités fédérales étant donné qu'une consultation est volontaire et ne peut empêcher la prise de mesures par les autorités fédérales (C.E., 9 décembre 2010, avis n° 48.989/VR, p.4).

Ce projet englobe les différents aspects de la résilience des entités critiques, leur protection et leur sécurité étant l'un des éléments déjà bien développés dans la loi IC. Ce qui a été construit dans le passé est ainsi préservé et intégré, tout en étendant la résilience à tous les risques contenus dans la directive CER, dont cette loi CER est la transposition.

Cette procédure d'identification s'effectue par l'application des critères définis ci-après.

Le deuxième paragraphe décrit la façon dont se déroule l'identification des infrastructures critiques gérées par

het beheer van de potentiële kritieke entiteiten. Het is de verantwoordelijkheid van de potentiële kritieke entiteit, die op grond van paragraaf 1 op de hoogte is van de lopende identificatieprocedure, om een lijst op te stellen van kritieke infrastructuren waarvan haar essentiële dienstverlening afhankelijk is.

De potentiële kritieke entiteit maakt de gemotiveerde lijst van kritieke infrastructuren binnen haar entiteit binnen zes maanden na de kennisgeving uit paragraaf 1 over aan de sectorale overheid. De sectorale overheid kan aan de potentiële kritieke entiteit bijsturingen opleggen in de voorgestelde lijst van kritieke infrastructuren, rekening houdend met de criteria die zij gebruikt tijdens de identificatieprocedure op grond van paragraaf 1, alsook met de coherentie in haar sector of deelsector voor wat betreft de identificatie van kritieke infrastructuren. De bevoegde sectorale overheid kan verduidelijking en toelichting vragen aan de potentiële kritieke entiteit en kan desgevallend voorgestelde kritieke infrastructuren weigeren dan wel andere infrastructuren binnen de kritieke entiteit aanduiden, mits opgave van redenen.

De kritieke entiteit is verantwoordelijk voor het actualiseren van deze lijst, en moet binnen een periode van 30 dagen na een wijziging van de lijst de bevoegde sectorale overheid op de hoogte stellen van deze wijzigingen. Dergelijke wijziging kan onder meer een adreswijziging, een toevoeging en een schrapping van een kritieke infrastructuur inhouden. De sectorale overheid stuurt deze informatie onverwijld door naar het NCCN.

Een goede informatie-uitwisseling tussen de sectorale overheden en potentiële kritieke entiteiten is noodzakelijk om dit proces vlot en kwaliteitsvol te laten verlopen. Om deze informatiestroom te faciliteren, werd in het huidige ontwerp een delegatie aan de Koning voorzien voor het opstellen van modaliteiten betreffende de informatie-uitwisseling.

Het Centrum voor Cybersecurity België (CCB) wordt tijdens het hele identificatieproces, bij het door de sectorale overheden en het NCCN gevoerde overleg, betrokken, binnen de grenzen van hun respectievelijke bevoegdheden, voor wat betreft de kritieke entiteiten die betrekking hebben op de beveiliging van netwerk- en informatiesystemen, dit omdat, behoudens tegenbewijs, de kritieke entiteiten geacht worden afhankelijk te zijn van netwerk- en informatiesystemen, en een goede informatie-uitwisseling hieromtrent tussen de bevoegde autoriteiten noodzakelijk is.

Gelet op het feit dat kritieke entiteiten op grond van de NIS 2-wet automatisch essentiële entiteiten zijn, wordt ook het CCB als de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de wet tot vaststelling

les entités critiques potentielles. Il appartient à l'entité critique potentielle qui, conformément au paragraphe 1er, est au courant de la procédure d'identification en cours, d'établir la liste des infrastructures critiques dont ses services essentiels dépendent.

L'entité critique potentielle transmet la liste motivée des infrastructures critiques de son entité à l'autorité sectorielle dans les six mois suivant la notification visée au paragraphe 1er. L'autorité sectorielle peut imposer à l'entité critique potentielle des ajustements à la liste d'infrastructures critiques proposée, en tenant compte des critères qu'elle utilise durant la procédure d'identification en vertu du paragraphe 1er, ainsi que de la cohérence dans son secteur ou sous-secteur en termes d'identification des infrastructures critiques. L'autorité sectorielle compétente peut demander des éclaircissements et des explications à l'entité critique potentielle et, le cas échéant, rejeter les infrastructures critiques proposées ou désigner d'autres infrastructures au sein de l'entité critique, en motivant sa décision.

L'entité critique est responsable de l'actualisation de cette liste et doit informer, dans une période de 30 jours après une modification de cette liste, l'autorité sectorielle compétente de cette modification. Une telle modification peut notamment concerner un changement d'adresse, un ajout et une suppression d'une infrastructure critique. L'autorité sectorielle transmet ces informations au NCCN dans les plus brefs délais.

Un échange efficace d'informations entre les autorités sectorielles et les entités critiques potentielles est nécessaire afin d'assurer un déroulement correct et qualitatif du processus. Pour faciliter ce flux d'informations, le présent projet prévoit une délégation au Roi afin d'établir les modalités de l'échange d'informations.

Tout au long du processus d'identification, le Centre pour la cybersécurité Belgique (CCB) est impliqué dans la concertation menée par les autorités sectorielles et le NCCN, dans les limites de leurs compétences respectives, pour ce qui concerne les entités critiques qui portent sur la sécurité des systèmes de réseau et d'information. La raison en est que, sauf preuve du contraire, les entités critiques sont supposées dépendre des systèmes de réseau et d'information, et qu'un bon échange d'informations à ce sujet est nécessaire entre les autorités compétentes.

Étant donné que les entités critiques sont automatiquement des entités essentielles en vertu de la loi NIS 2, le CCB, en tant qu'autorité nationale de cybersécurité visée à l'article 16 de la loi établissant un cadre pour la

van een kader voor de cyberbeveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid, geïnformeerd van de aanduidingen van kritieke entiteiten.

Art. 11

Artikel 11 houdt de omzetting in van artikel 6 van de CER-Richtlijn, waarin de drie basiscriteria vastgelegd worden waaraan een entiteit moet voldoen alvorens deze kan geïdentificeerd worden als kritieke entiteit.

Tijdens de identificatieprocedure moeten de sectorale overheden ten minste rekening houden met deze criteria aan de hand waarvan kan worden bepaald hoe ernstig het verstorend effect van een incident is of kan zijn, welke één van de drie basiscriteria is. Deze criteria worden omschreven in artikel 7 paragraaf 1 van de CER-Richtlijn. Het komt aan de sectorale overheid toe om, in het kader van de identificatie van de kritieke entiteiten de niveaus van weerslag of de drempelwaarden van deze criteria te definiëren. De sectorale overheid kan daarnaast bijkomend de criteria aanvullen met sector of deelsectorspecifieke eigenschappen.

Deze criteria worden zo veel als mogelijk op kwantitatieve en (deel-)sectorspecifieke wijze bepaald en gemotiveerd. Een duidelijke en kwaliteitsvolle redenering is van essentieel belang voor het verdere verloop van het identificatieproces. Het NCCN kan, aan de hand van een gemotiveerd verzoek, alle relevante informatie hierover opvragen zodat onder meer het advies uit artikel 13 van dit ontwerp correct onderbouwd kan worden.

De sectorale overheid bepaalt de niveaus van weerslag of de drempelwaarden van deze criteria, in overleg met het NCCN, en in voorkomend geval, na raadpleging van de gefedereerde entiteiten voor zover het gaat om hun bevoegdheden. In dit verband wordt verwezen naar het commentaar betreffende artikel 10, § 1.

Het overleg met het NCCN, wat betreft de criteria uit artikel 11 van dit ontwerp, is gerechtvaardigd door haar coördinatierol op het vlak van de weerbaarheid van de kritieke entiteiten. Dat overleg moet een harmonisering van de benaderingswijze binnen de verschillende sectoren mogelijk maken.

Art. 12

Na de kritieke entiteiten te hebben geïdentificeerd, moet de sectorale overheid overgaan tot hun aanduiding.

cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est également informée des désignations d'entités critiques.

Art. 11

L'article 11 est une transposition de l'article 6 de la directive CER, qui définit les trois critères de base auxquels une entité doit satisfaire avant de pouvoir être identifiée comme entité critique.

Durant le processus d'identification, l'autorité sectorielle doit au moins tenir compte de ces critères qui permettent de déterminer le degré de gravité de l'impact perturbateur qu'a ou peut avoir un incident, ce qui constitue l'un des trois critères de base. Ces critères sont définis à l'article 7, paragraphe 1, de la directive CER. Il appartient à l'autorité sectorielle de définir, dans le cadre de l'identification des entités critiques, les niveaux d'impact ou les valeurs seuils de ces critères. L'autorité sectorielle peut compléter les critères par des caractéristiques spécifiques au secteur ou au sous-secteur.

Dans la mesure du possible, ces critères sont déterminés et justifiés d'une manière quantitative et (sous-) sectorielle. Un raisonnement clair et de qualité est essentiel pour la suite du processus d'identification. À tout moment, le NCCN peut, sur requête motivée, demander toutes les informations pertinentes à ce sujet afin de pouvoir correctement étayer, entre autres, l'avis prévu à l'article 13 du présent projet.

L'autorité sectorielle détermine les niveaux d'impact ou les valeurs seuils de ces critères en concertation avec le NCCN et, le cas échéant, après consultation des entités fédérées pour autant qu'il s'agisse de leurs compétences. Il est fait référence à cet égard au commentaire relatif à l'article 10, § 1er.

La concertation avec le NCCN, en ce qui concerne les critères de l'article 11 du présent projet, est justifiée par le rôle de coordination du NCCN en matière de résilience des entités critiques. Cette concertation doit permettre une harmonisation de l'approche au sein des différents secteurs.

Art. 12

Après avoir identifié les entités critiques, l'autorité sectorielle doit procéder à leur désignation.

Paragraaf 1 omschrijft het mechanisme voor de aanduiding van de kritieke entiteiten en kritieke infrastructuren, namelijk de aanduiding na het advies van het NCCN. Het advies wordt gegeven nadat een geconsolideerd dossier werd bezorgd aan het NCCN, waarin alle nodige informatie staat dat nodig kan zijn om een grondig gemotiveerd advies te kunnen geven. Dat advies is gerechtvaardigd door de coördinatierol van het NCCN, beschreven in het commentaar bij artikel 11. Dit advies is niet bindend voor de sectorale overheid, maar heeft wel een belangrijke adviserende waarde.

Het NCCN zal voor elke substantiële wijziging in het geconsolideerde dossier opnieuw advies moeten geven over die wijziging. Met een substantiële wijziging wordt bedoeld een toevoeging of schrapping van kritieke infrastructuur, en niet de loutere adreswijziging van bestaande kritieke infrastructuur. Dit advies heeft als doel de harmonisatie tussen de sectoren te waarborgen.

Bij afwezigheid van aanduiding van een kritieke entiteit in haar welbepaalde (deel)sector, zet de bevoegde sectorale overheid hiervoor de redenen uiteén die geleid hebben tot deze afwezigheid. Deze motivatie kan bestaan uit de toetsing van de criteria uit artikel 11, § 1 en § 2.

Artikel 6.5. van de Richtlijn bepaalt dat het identificatie- en aanduiding proces ten minste elke vier jaar, en telkens wanneer nodig, hernieuwd wordt.

Indien een kritieke entiteit niet meer voldoet aan de criteria uit artikel 11, dan kan zij niet meer aangeduid blijven als zodanig. De sectorale overheid stelt de entiteit in kennis dat zij niet meer moet voldoen aan de verplichtingen uit de wet.

Art. 13

Artikel 13 bepaalt de vormvoorschriften voor de aanduiding van de kritieke entiteit, namelijk de betekening van de gemotiveerde beslissing ter aanduiding aan de kritieke entiteit.

Het is belangrijk dat men precies kan bepalen op welke datum de betekening van de aanduiding is gebeurd, omdat dat het startpunt is voor de termijn voor de verplichtingen van de kritieke entiteit, die zijn beschreven in het commentaar van de artikelen 16 tot 20 van deze wet.

In de KI-wet werd enkel de burgemeester van de gemeente op het grondgebied waarvan de kritieke entiteit zich bevindt, op de hoogte gebracht van deze aanduiding, in het kader van de externe bescherming. Op grond van de CER-Richtlijn moeten de weerbaarheidsplannen nu

Le paragraphe 1er définit le mécanisme de désignation des entités critiques et des infrastructures critiques, à savoir la désignation après l'avis du NCCN. L'avis est rendu après transmission d'un dossier consolidé au NCCN qui contient toutes les informations pouvant être nécessaires pour rendre un avis dûment motivé. Cet avis est justifié par le rôle de coordination du NCCN, tel que décrit au commentaire de l'article 11. Il n'est pas contraignant pour l'autorité sectorielle, mais il a une importante valeur consultative.

Le NCCN devra rendre un nouvel avis pour chaque modification substantielle apportée au dossier consolidé au sujet de cette modification. Par modification substantielle, on entend un ajout ou une suppression de l'infrastructure critique et non pas un simple changement d'adresse. Cet avis vise à garantir l'harmonisation entre les secteurs.

En l'absence de désignation d'une entité critique dans son (sous-)secteur déterminé, l'autorité sectorielle compétente expose les motifs qui ont conduit à cette absence. Cette motivation peut consister en l'examen des critères repris à l'article 11, § 1er et § 2.

L'article 6.5. de la directive stipule que le processus d'identification et de désignation est renouvelé au moins tous les quatre ans, et chaque fois que cela s'avère nécessaire.

Si une entité critique ne répond plus aux critères de l'article 11, elle ne peut plus être désignée comme telle. L'autorité sectorielle notifie à l'entité qu'elle n'est plus tenue de remplir les obligations prévues par la loi.

Art. 13

L'article 13 détermine les prescriptions de forme pour la désignation de l'entité critique, à savoir la notification de la décision motivée de désignation à l'entité critique.

Il est important de pouvoir déterminer avec précision la date de la notification de la désignation, car il s'agit du point de départ du délai pour les obligations de l'entité critique, qui sont décrites dans le commentaire des articles 16 à 20 de la présente loi.

Dans la loi IC, seul le bourgmestre de la commune sur le territoire de laquelle se trouve l'entité critique était informé de cette désignation, dans le cadre de la protection externe. En vertu de la directive CER, les plans de résilience doivent désormais également inclure des

ook verplicht interne noodplannen bevatten, waardoor logischerwijze de gouverneurs mee in kennis gesteld moeten worden, zodat zij hun externe noodplannen hierop kunnen afstemmen. Gelet op het feit dat men ook op gemeentelijk niveau externe noodplannen kan opstellen, zal de burgemeester tevens ingelicht worden in die hoedanigheid.

Er zal moeten bepaald worden of de kennis over de ligging van de kritieke entiteit aanpassingen of aanvullingen vereisen aan het bestaande algemene nood- en interventieplan (ANIP) en bijzonder nood- en interventieplan (BNIP). De gouverneur kan bepalen, op basis van het uitvoeren van een risicobeoordeling, of de externe noodplanning idealiter uitgevoerd wordt op gemeentelijk of provinciaal niveau. Deze wet doet geen afbreuk aan de algemene reglementering inzake de externe noodplanning, die haar oorsprong vindt in artikel 9 van de wet van 15 mei 2007 betreffende de civiele veiligheid en bijhorende uitvoeringsbesluiten.

De burgermeesters en gouverneurs die op de hoogte gesteld worden van dergelijke aanduiding dienen deze inherent gevoelige informatie te behandelen volgens het principe van de beperkte verspreiding, en mogen deze enkel delen met personen die ervan kennis nodig hebben voor de uitoefening van hun beroep in het proces van de externe noodplanning, zoals bedoeld in artikel 28 en 29 van deze wet.

Wanneer er informatie in verband met kritieke entiteiten wordt toegevoegd aan een ANIP of wanneer er een afzonderlijk BNIP geschreven wordt, dient men ook op het nationaal veiligheidsportaal het *need-to-know* principe te respecteren.

Wanneer de aanduiding van een kritieke entiteit meerdere sectoren of deelsectoren aanbelangt, kan het NCCN, in uitvoering van haar coördinerende opdracht, de bevoegde sectorale overheden samenbrengen voor overleg tussen de sectorale overheden zodat er voor de kritieke entiteiten geen dubbele verplichtingen bestaan. Tijdens het facultatieve overleg kunnen bijvoorbeeld afspraken gemaakt worden met betrekking tot de inspecties en audits. Aangezien in verschillende sectoren de minister aangeduid wordt als sectorale overheid, zal deze ook op de hoogte gesteld kunnen worden van de aanduidingen door de administraties die onder zijn of haar bevoegdheden vallen. De voorzitter van de Nationale Autoriteit voor Maritieme Beveiliging (NAMB) wordt tevens ingelicht van aanduidingen in het Belgisch gedeelte van de Noordzee.

plans d'urgence internes, ce qui nécessite logiquement que les gouverneurs soient également informés, de sorte à pouvoir aligner leurs plans d'urgence externes en conséquence. Étant donné qu'il est également possible d'élaborer des plans d'urgence externes au niveau communal, le bourgmestre sera également informé à ce titre.

Il faudra déterminer si la connaissance de l'emplacement de l'entité critique nécessite des ajustements ou des ajouts aux plan général d'urgence et d'intervention (PGUI) et plan particulier d'urgence et d'intervention (PPUI) existants. Le gouverneur peut déterminer, sur la base d'une évaluation des risques, si les plans d'urgence externes devraient idéalement être mis en œuvre au niveau communal ou provincial. Cette loi n'affecte pas la réglementation générale relative aux plans d'urgence externes, qui trouve son origine dans l'article 9 de la loi du 15 mai 2007 relative à la sécurité civile et ses arrêtés d'exécution.

Les bourgmestres et les gouverneurs informés de cette désignation traitent ces informations intrinsèquement sensibles selon le principe de la diffusion restreinte et ne peuvent les partager qu'avec les personnes qui ont besoin d'en avoir connaissance pour l'exercice de leur profession dans le cadre du processus de planification d'urgence externe, tel que visé aux articles 28 et 29 de la présente loi.

Lorsque des informations critiques relatives à une entité sont ajoutées à un PGUI ou qu'un PPUI distinct est rédigé, le principe du besoin d'en connaître doit également être respecté sur le portail de sécurité national.

Lorsque la désignation d'une entité critique concerne plusieurs secteurs ou sous-secteurs, le NCCN peut, dans le cadre de sa mission de coordination, réunir les autorités sectorielles compétentes pour une consultation entre les autorités sectorielles afin d'éviter la duplication des obligations des entités critiques. Au cours de cette concertation facultative, des accords peuvent être conclus sur les inspections et les audits, par exemple. Étant donné que, dans plusieurs secteurs, le ministre est désigné comme autorité sectorielle, il pourra également être informé des désignations effectuées par les administrations relevant de sa compétence. Le président de l'Autorité Nationale de Sûreté Maritime (ANSM) est également informé des désignations dans la partie belge de la mer du Nord.

Afdeling 2

Kritieke entiteiten van Europees belang

Art. 14

Dit artikel beschrijft de identificatieprocedure van kritieke entiteiten van bijzonder Europees belang, en zet hoofdstuk IV van de CER-Richtlijn om. Ofschoon kritieke entiteiten over het algemeen binnen een steeds hechter dienstverlenings- en infrastructureel netwerk opereren en dikwijls in meer dan één lidstaat essentiele diensten verlenen, zijn een aantal van die kritieke entiteiten van bijzonder belang voor de Unie omdat zij essentiële diensten verlenen aan of in ten minste zes lidstaten, en kunnen zij daarom specifieke ondersteuning op Unieniveau krijgen.

De entiteit die werd aangeduid als kritieke entiteit op grond van artikel 13 van deze wet, is verantwoordelijk om de bevoegde sectorale overheid te informeren in het geval zij essentiële diensten verleent aan of in meer dan zes lidstaten. De kritieke entiteit vermeldt hierbij over welke essentiële diensten het gaat en in welke lidstaten deze worden verleend. Het NCCN stelt, in haar functie als Nationaal Centraal Contactpunt, in overleg met de bevoegde sectorale overheden, zonder onnodige vertraging de Europese Commissie in kennis van de identiteit van dergelijke kritieke entiteiten en van de informatie die zij verstrekken op basis van dit artikel.

De Commissie raadpleegt via het Nationaal Centraal Contactpunt de bevoegde sectorale overheid, die de kritieke entiteit als zodanig heeft aangeduid, de bevoegde autoriteit van andere betrokken lidstaten en de betrokken kritieke entiteit zelf. Deze raadpleging heeft als doel te onderzoeken of de geleverde diensten wel degelijk als essentiële diensten zijn aangeduid in de betrokken lidstaten. In het geval dat de Commissie oordeelt dat de betrokken kritieke entiteit essentiële diensten verleent aan of in meer dan zes lidstaten, stelt zij het NCCN ervan in kennis dat de entiteit als een kritieke entiteit van bijzonder Europees belang wordt beschouwd. Het NCCN stelt onverwijld de bevoegde sectorale overheid hiervan in kennis, dewelke op haar beurt de kritieke entiteit zonder onnodige vertraging de kennisgeving toezendt.

De bepalingen onder hoofdstuk 5 van dit ontwerp zijn van toepassing vanaf de datum van ontvangst door de kritieke entiteit van de kennisgeving door de sectorale overheid dat zij als kritieke entiteit van Bijzonder Europees Belang beschouwd wordt.

Section 2

Entités critiques revêtant une importance européenne particulière

Art. 14

Cet article décrit la procédure d'identification des entités critiques revêtant une importance européenne particulière et transpose le chapitre IV de la directive CER. Bien que les entités critiques opèrent en général au sein d'un réseau toujours plus dense de services et d'infrastructures et fournissent souvent des services essentiels dans plus d'un État membre, un certain nombre d'entre elles revêtent une importance particulière pour l'Union parce qu'elles fournissent des services essentiels à ou dans six États membres ou plus, et peuvent par conséquent recevoir un soutien spécifique au niveau de l'Union.

L'entité qui a été désignée comme entité critique en vertu de l'article 13 de la présente loi est chargée d'informer l'autorité sectorielle compétente dans le cas où elle fournit des services essentiels à ou dans six États membres ou plus. L'entité critique mentionne de quels services essentiels il s'agit et dans quels États membres ceux-ci sont fournis. Le NCCN, en sa qualité de Point de Contact Central National, en consultation avec les autorités sectorielles compétentes, notifie sans délai la Commission européenne de l'identité de ces entités critiques et des informations qu'elles fournissent sur la base du présent article.

La Commission consulte via le Point de Contact Central National l'autorité sectorielle compétente, qui a désigné l'entité critique comme telle, l'autorité compétente d'autres États membres concernés ainsi que l'entité critique concernée. Cette consultation vise à examiner si les services fournis ont bel et bien été désignés comme services essentiels dans les États membres concernés. Dans le cas où la Commission estime que l'entité critique concernée fournit des services essentiels à six États membres ou plus, elle communique au NCCN que l'entité est considérée comme une entité critique revêtant une importance européenne particulière. Le NCCN informe sans délai l'autorité sectorielle compétente qui envoie à son tour, sans délai, la notification à l'entité critique.

Les dispositions du chapitre 5 du présent projet s'appliquent à partir de la date de réception, par l'entité critique, de la notification par l'autorité sectorielle selon laquelle elle est considérée comme une entité critique revêtant une importance européenne particulière.

In overleg met de lidstaat die de kritieke entiteit van bijzonder Europees belang heeft geïdentificeerd als een kritieke entiteit, moet de Commissie een adviesmissie kunnen organiseren om de door die entiteit genomen maatregelen te beoordelen.

Art. 15

Het NCCN, in haar functie van Nationaal Centraal Contactpunt, vervult een verbindingsfunctie met het oog op grensoverschrijdende samenwerking met de centrale contactpunten van de andere lidstaten. Artikel 15 beschrijft de mogelijkheid om bilaterale of multilaterale besprekingen te voeren met betrokken lidstaten van de Europese Unie in het geval dat een kritieke entiteit op Belgisch grondgebied banden heeft met die lidstaten, doordat er gebruik gemaakt wordt van kritieke infrastructuur die verbonden is tussen twee of meer lidstaten, doordat zij deel uitmaken van bedrijfsstructuren die verbonden zijn aan kritieke entiteiten in andere lidstaten of wanneer zij essentiële diensten verlenen aan of in andere lidstaten. Met name worden hier de kritieke entiteiten bedoeld die niet voldoen aan de voorwaarden om als kritieke entiteiten van Bijzonder Europees Belang aangeduid te worden, en dus geen essentiële diensten verlenen aan of in meer dan zes lidstaten. De bevoegde sectorale overheid informeert het centraal contactpunt tijdens de identificatieprocedure of een kritieke entiteit in haar sector of deelsector valt onder dit artikel.

Dit artikel komt tegemoet aan het wegvallen van de categorie “Europese Kritieke Infrastructuur” uit de ECI-Richtlijn. De entiteiten die voorheen als zodanig werden geïdentificeerd, maar onder dit ontwerp niet voldoen aan de drempel van zes lidstaten, zullen voortaan geen bijzonder statuut meer bezitten. Dit artikel benadrukt voor deze gevallen de mogelijkheid tot bilaterale of multilaterale samenwerking.

HOOFDSTUK 5

Interne weerbaarheidsmaatregelen van kritieke entiteiten

Art. 16

In dit hoofdstuk worden de weerbaarheidsmaatregelen georganiseerd die de kritieke entiteit moet nemen, in functie van de risico’s waaraan zij wordt blootgesteld.

Artikel 13.3 van de CER-Richtlijn legt de verplichting op aan de kritieke entiteit om een “Contactpunt kritieke entiteit” aan te duiden, die een rol van contactpunt vervult

En concertation avec l’État membre qui a identifié l’entité critique revêtant une importance européenne particulière comme entité critique, la Commission doit pouvoir organiser une mission de conseil afin d’évaluer les mesures prises par cette entité.

Art. 15

En sa qualité de Point de Contact Central National, le NCCN remplit une fonction de liaison en vue de la collaboration transfrontalière avec les points de contact centraux des autres États membres. L’article 15 décrit la possibilité de mener des discussions bilatérales ou multilatérales avec les États membres concernés de l’Union européenne au cas où une entité critique a, sur le territoire belge, des liens avec ces États membres parce qu’elle utilise des infrastructures critiques physiquement connectées entre deux États membres ou plus, qu’elles font partie de structures d’entreprise liées à des entités critiques dans d’autres États membres ou quand elles fournissent des services essentiels à ou dans d’autres États membres. Sont ici visées les entités critiques qui ne répondent pas aux conditions pour être désignées comme entités critiques revêtant une importance européenne particulière et qui ne fournissent donc pas de services essentiels à ou dans six États membres ou plus. L’autorité sectorielle compétente indique au point de contact central, au cours de la procédure d’identification, si une entité critique de son secteur ou sous-secteur est visée par le présent article.

Cet article tient compte de la suppression de la catégorie des “Infrastructures Critiques Européennes” de la directive ICE. Les entités précédemment identifiées comme telles, mais qui, selon ce projet, n’atteignent pas le seuil de six États membres, ne bénéficieront désormais plus d’un statut spécial. Dans de tels cas, cet article souligne la possibilité d’une coopération bilatérale ou multilatérale.

CHAPITRE 5

Mesures internes de la résilience des entités critiques

Art. 16

Ce chapitre régit les mesures de résilience que l’entité critique doit prendre, en fonction des risques auxquels elle est exposée.

L’article 13.3 de la Directive CER impose à l’entité critique l’obligation de désigner un “Point de Contact entité critique”, qui joue le rôle de point de contact avec

met de bevoegde overheden. Dergelijke verplichting stond ook in de KI-wet, en houdt dus een verderzetting in van het beleid hieromtrent.

Omdat het doel hiervan het verzekeren van een permanent contactpunt is tussen de kritieke entiteit en de autoriteiten, werd gekozen voor een contactpunt dat 24u/24bereikbaar is voor de bevoegde autoriteiten, het NCCN, de burgemeester en de gouverneur. Het is aan de entiteit om toe te zien dat er permanentie verzekerd wordt door één of verschillende personen bevoegd om de veiligheidsvragen met betrekking tot de kritieke entiteiten te behandelen.

De kritieke entiteit dient dit contactpunt aan te duiden en de contactgegevens te communiceren binnen de zes maanden van zijn aanduiding als kritieke entiteit.

Het derde lid beoogt de hypothese waarin een contactpunt van hetzelfde type reeds opgelegd zou zijn aan de kritieke entiteit krachtens andere nationale of internationale reglementeringen.

Dit is momenteel het geval voor wat betreft de havens, die op grond van de wet van 8 mei 2019 tot invoering van het Belgisch Scheepvaartswetboek, een maritieme beveiligingsfunctionaris moeten aanduiden, dewelke fungeert als lokaal contactpersoon voor alle aangelegenheden die verband houden met de maritieme beveiliging van de betrokken haven.

De laatste lid van dit artikel legt een beschikbaarheid op aan het contactpunt van 24u/24, aangezien een incident zich op elk ogenblik kan voordoen.

Art. 17

Artikel 12.1 van de Richtlijn legt op dat de kritieke entiteiten alle relevante risico's beoordelen die de verlening van hun essentiële diensten kunnen verstoren.

Kritieke entiteiten moeten een breed inzicht hebben in de risico's waaraan zij blootgesteld kunnen worden en zij moeten deze risico's afdoende analyseren. Daartoe moeten zij, telkens wanneer hun specifieke omstandigheden en de evolutie van die risico's daartoe nopen, en in ieder geval om de vier jaar, risicobeoordelingen uitvoeren. Hierbij moet tevens rekening gehouden worden met afhankelijkheden binnen en van andere in deze wet genoemde sectoren, en in voorkomend geval ook in naburige lidstaten en derde landen.

De sectorale overheid dient zijn sectorale risicobeoordeling, uitgevoerd op basis van artikel 8 van dit ontwerp,

les autorités compétentes. Cette obligation figurait également dans la loi IC et représente donc une continuation de la politique en la matière.

Dans la mesure où l'objectif est d'assurer un point de contact permanent entre l'entité critique et les autorités, il a été décidé d'opter pour un point de contact disponible 24h/24 pour les autorités compétentes, le NCCN, le bourgmestre et le gouverneur. Il appartient à l'entité de veiller à ce qu'une permanence soit assurée par une ou plusieurs personnes compétentes pour traiter les questions de sécurité relatives aux entités critiques.

L'entité critique est tenue de désigner ce point de contact et de communiquer les coordonnées de contact endéans les six mois de sa désignation comme entité critique.

L'alinéa 3 vise l'hypothèse dans laquelle un point de contact du même type aurait déjà été imposé à l'entité critique en vertu d'autres réglementations nationales ou internationales.

Ceci est actuellement le cas en ce qui concerne les ports qui, conformément à la loi du 8 mai 2019 introduisant le Code belge de la Navigation, sont tenus de désigner un agent de sûreté maritime qui agit en tant que personne de contact locale pour toutes les questions liées à la sécurité maritime du port concerné.

Le dernier alinéa de cet article impose au point de contact une disponibilité 24h/24 étant donné qu'un incident peut survenir à tout instant.

Art. 17

L'article 12.1 de la directive impose aux entités critiques d'évaluer tous les risques pertinents susceptibles de perturber la fourniture de leurs services essentiels.

Les entités critiques doivent avoir une connaissance approfondie des risques auxquels elles peuvent être exposées et elles doivent les analyser de façon adéquate. À cette fin, elles doivent procéder à des évaluations des risques chaque fois que leurs circonstances particulières et l'évolution de ces risques l'exigent et, en tout cas, tous les quatre ans. Il faut également tenir compte à cet égard des dépendances au sein de et émanant d'autres secteurs cités dans la présente loi et, le cas échéant, dans les États membres voisins et les pays tiers.

L'autorité sectorielle est tenue de communiquer à l'entité critique son évaluation sectorielle des risques,

mee te delen aan de kritieke entiteit zodat deze de relevante informatie hieruit kan opnemen in zijn eigen risicobeoordeling. Hiernaast houdt de kritieke entiteit ook rekening met de dreigingsanalyse uitgevoerd op basis van artikel 9, en alle andere relevante informatie waarover zij beschikt.

Indien kritieke entiteiten risicobeoordelingen hebben uitgevoerd of documenten hebben opgesteld op grond van verplichtingen opgenomen in andere rechtshandelingen, die relevant zijn voor hun risicobeoordeling, kunnen zij die beoordelingen en documenten gebruiken om aan de voorschriften voor hun risicobeoordeling die zijn vastgesteld in deze wet, te voldoen.

Art. 18

Dit artikel legt aan de kritieke entiteit de verplichting op om een weerbaarheidsplan van de kritieke entiteit (hieronder "W.P.E.") uit te werken die de technische, beveiligings- en organisatorische weerbaarheidsmaatregelen bevat, om incidenten te voorkomen, te beperken of te beheersen, en om bescherming te bieden of bestand te zijn tegen, te reageren op of zich aan te passen aan een incident of daarvan te herstellen. Deze weerbaarheidsmaatregelen moeten in verhouding en evenredig zijn met de verschillende risico's die elke kritieke entiteit bij haar risicobeoordeling heeft vastgesteld en de specifieke kenmerken van de betrokken entiteit.

Het W.P.E. moet weerbaarheidsmaatregelen bevatten die toegepast worden in functie van de risico's waaraan de entiteit kan worden blootgesteld, rekening houdend met de mogelijkheid tot wijzigende omstandigheden. Dit wil zeggen dat er naast de standaard maatregelen ook de mogelijkheid moet zijn om de maatregelen op te schalen wanneer de omstandigheden hiertoe noodzaken. Een opschaling van maatregelen kan bijvoorbeeld nodig zijn in het geval van een concrete dreiging, noodweer of een gezondheidscrisis. De kritieke entiteit is verantwoordelijk voor het bepalen welke maatregelen adequaat en noodzakelijk worden geacht om tegemoet te komen aan veranderende omstandigheden.

Voor het overige is de mogelijkheid gelaten aan de Koning om eventuele aanvullende informatie of maatregelen die het W.P.E. moet bevatten voor een bepaalde sector, of voor een deelsector, vast te leggen. De specificiteit van de ene of de andere sector kan immers verantwoorden dat de sectorale overheid gemeenschappelijke richtlijnen op het vlak van weerbaarheidsmaatregelen vastlegt. De wet bepaalt aldus de algemene verplichtingen waaraan bijzondere verplichtingen die eigen zijn aan elke sector kunnen worden toegevoegd.

menée sur la base de l'article 8 du présent projet, afin de lui permettre d'intégrer les informations pertinentes dans sa propre évaluation des risques. En outre, l'entité critique tient également compte de l'analyse de la menace effectuée en vertu de l'article 9, et de toutes les autres informations pertinentes dont elle dispose.

Si les entités critiques ont effectué des évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour leurs évaluations des risques, elles peuvent utiliser ces évaluations et documents pour répondre aux prescriptions concernant leurs évaluations des risques contenues dans la présente loi.

Art. 18

Cet article impose à l'entité critique l'obligation d'élaborer un plan de résilience de l'entité critique (ci-après dénommé "P.R.E.") qui contient les mesures techniques, de sécurité et organisationnelles de résilience en vue de prévenir tout incident, de le limiter ou de le maîtriser, et de s'en protéger ou d'y résister, d'y réagir, de s'y adapter ou de s'en rétablir. Ces mesures de résilience doivent être appropriées et proportionnées aux différents risques que chaque entité critique a identifiés dans son évaluation des risques, ainsi qu'aux spécificités de l'entité concernée.

Le P.R.E. doit contenir des mesures de résilience qui s'appliquent en fonction des risques auxquels l'entité peut être exposée, compte tenu de la possibilité d'un changement de circonstances. Cela signifie qu'outre les mesures standard, il doit également être possible de renforcer les mesures quand les circonstances le nécessitent. Un renforcement des mesures peut s'avérer nécessaire, par exemple, en cas de menace concrète, de conditions météorologiques défavorables ou de crise sanitaire. L'entité critique est chargée de déterminer les mesures jugées adéquates et nécessaires pour faire face à l'évolution de la situation.

Pour le surplus, le Roi a la possibilité de prévoir des informations ou mesures complémentaires éventuelles que le P.R.E. doit contenir pour un secteur ou un sous-secteur déterminé. La spécificité d'un secteur ou d'un autre peut en effet justifier que l'autorité sectorielle définisse des orientations communes en ce qui concerne les mesures de résilience. La loi fixe dès lors les obligations générales auxquelles des obligations particulières, propres à chaque secteur, peuvent être ajoutées.

De tweede paragraaf bevat de weerbaarheidsmaatregelen die het W.P.E. minstens moet bevatten, om te voldoen aan de verplichtingen uit de CER-Richtlijn.

Voor wat betreft de maatregelen uit punt c), wordt hiermee bedoeld de informatie die ter beschikking moet gesteld worden aan de burgemeester en/of gouverneur wanneer zij besluiten te werken aan externe noodplanning.

Met het oog op effectiviteit en verantwoording moeten kritieke entiteiten, rekening houdend met de vastgestelde risico's, de maatregelen die zij nemen voldoende gedetailleerd beschrijven in het W.P.E., dan wel een of meer daarmee vergelijkbare documenten, teneinde dat plan in de praktijk toe te passen.

De weerbaarheidsmaatregelen voorgeschreven door het W.P.E. moeten geïmplementeerd worden binnen een termijn van maximum 10 maanden vanaf de aanduiding als kritieke entiteit.

De kritieke entiteit, als eerste verantwoordelijke voor de weerbaarheid van zijn entiteit en bijhorende kritieke infrastructuur, draagt dus de verantwoordelijkheid voor het uitwerken van het W.P.E. en het implementeren van de hierin opgenomen weerbaarheidsmaatregelen.

Wanneer een kritieke entiteit reeds technische-, beveiligings- en organisatorische maatregelen heeft genomen en documenten heeft opgesteld op grond van andere rechtshandelingen die relevant zijn voor weerbaarheidsbevorderende maatregelen uit hoofde van deze wet, moet zij die maatregelen en documenten kunnen gebruiken om aan de voorschriften ten aanzien van de weerbaarheidsmaatregelen uit hoofde van de wet te voldoen. Om dubbel werk te voorkomen kunnen bestaande weerbaarheidsmaatregelen genomen door de kritieke entiteit, die geheel of ten dele voldoen aan de voorschriften van deze wet, gebruikt worden om te voldoen aan de voorwaarden uit artikel 18.

Wanneer een kritieke entiteit beschikt over een *Business Impact Analysis* (BIA) en/of een *Business Continuity Plan* (BCP), dan kan moet men deze kunnen gebruiken om te voldoen aan de voorwaarden uit artikel 18.

Krachtens paragraaf 5 moet de kritieke entiteit daarnaast oefeningen organiseren om het W.P.E. te testen en regelmatig te evalueren. De Koning kan de frequentie van de oefeningen en van de updates bepalen. De bepaalde termijn houdt aldus rekening met de realiteit van de sector of deelsector en van de frequentie die het meest geschikt is, en die per sector of deelsector anders kan zijn.

Le second paragraphe contient les mesures de résilience que le P.R.E. doit au moins contenir afin de répondre aux obligations prévues par la directive CER.

En ce qui concerne les mesures visées au point c), il s'agit des informations à mettre à la disposition du bourgmestre et/ou du gouverneur lorsqu'ils décident de travailler sur les plans d'urgence externes.

Dans un souci d'efficacité et de justification, compte tenu des risques identifiés, les entités critiques doivent décrire les mesures qu'elles prennent de façon suffisamment détaillée dans le P.R.E., ou dans un ou plusieurs documents similaires afin d'appliquer ce plan dans la pratique.

Les mesures de résilience prescrites par le P.R.E. doivent être mises en œuvre dans un délai de 10 mois maximum à compter de la désignation en tant qu'entité critique.

En tant que première responsable de la résilience de son entité et de l'infrastructure critique correspondante, l'entité critique est ainsi responsable de l'élaboration du P.R.E. et de la mise en œuvre des mesures de résilience qui y sont reprises.

Lorsqu'une entité critique a déjà pris des mesures techniques, de sécurité et organisationnelles et établi des documents en vertu d'autres actes juridiques qui sont pertinents pour les mesures de résilience prévues par la présente loi, elle doit pouvoir utiliser ces mesures et documents pour se conformer aux exigences relatives aux mesures de résilience prévues par la présente loi. Pour éviter tout double emploi, les mesures de résilience existantes prises par l'entité critique, qui sont conformes en tout ou en partie aux exigences de la présente loi, peuvent être utilisées pour remplir les conditions énoncées à l'article 18.

Si une entité critique dispose d'une *Business Impact Analysis* (BIA) et/ou d'un *Business Continuity Plan* (BCP), elle devrait avoir la possibilité de les utiliser pour remplir les conditions de l'article 18.

En vertu du paragraphe 5, l'entité critique doit organiser en outre des exercices afin de tester le P.R.E. et de l'évaluer régulièrement. Le Roi peut déterminer la fréquence des exercices et des mises à jour. Le délai fixé tient donc compte de la réalité du secteur ou sous-secteur et de la fréquence la plus appropriée, laquelle peut varier selon le secteur ou sous-secteur.

Delegatie wordt eveneens gegeven aan de Koning teneinde de nadere regels vast te stellen volgens dewelke alle bevoegde diensten, deelnemen aan de oefeningen georganiseerd door de kritieke entiteit.

De verplichtingen van de kritieke entiteit voor wat betreft de weerbaarheidsmaatregelen zijn in principe van toepassing op elke kritieke infrastructuur die zij geïdentificeerd hebben. Gelet op de uitvoerbaarheid van de oefeningen, volstaat het dat deze uitgevoerd worden op het niveau van kritieke entiteit. Deze oefeningen hebben betrekking op het type risico's waarmee de kritieke entiteit in aanraking kan komen, waarvoor het mogelijk is om oefeningen op te stellen.

Art. 19

Het risico bestaat dat werknemers van kritieke entiteiten of hun contractanten bijvoorbeeld hun toegangsrechten misbruiken om binnen de organisatie van de kritieke entiteit schade te veroorzaken. In artikel 14 van de CER-Richtlijn wordt daarom in de mogelijkheid tot een antecedentenonderzoek voorzien. Deze mogelijkheid bestaat reeds in België op grond van artikel 27 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst. Artikel 19 verduidelijkt dat voor de kritieke entiteiten die vallen onder het toepassingsgebied van deze wet, de sectorale overheid kan verzoeken dat een veiligheidsverificatie wordt uitgevoerd in overeenstemming met bovenvermelde wet. Artikel 19 laat de toepassing van de wet van 11 december 1998 dus onverlet. Aan de hand daarvan kan worden nagegaan of er voor een kritieke entiteit overgegaan moet worden tot het uitvoeren van veiligheidsverificaties voor het betrokken personeel.

Dit artikel laat de sectorspecifieke regelingen die hierrond reeds bestaan onverlet.

Art. 20

Krachtens dit artikel heeft de kritieke entiteit de verplichting om de incidenten die van aard zijn de verlening van essentiële diensten aanzienlijk te verstoren, te notifiëren, zodat de bevoegde overheden snel en adequaat kunnen reageren op incidenten en een volledig overzicht krijgen van de impact, aard, oorzaak en mogelijke gevolgen van incidenten waarmee kritieke entiteiten te maken hebben, en in voorkomend geval de meest geschikte externe beschermingsmaatregelen zouden kunnen nemen.

Une délégation est également donnée au Roi pour définir les modalités selon lesquelles les services compétents chargés, en vertu de la présente loi, de la mise en œuvre des mesures de protection externes, participent aux exercices organisés par l'entité critique.

Les obligations de l'entité critique en matière de mesures de résilience sont en principe applicables à toute infrastructure critique qu'elle a identifiée. Compte tenu de la faisabilité des exercices, il suffit qu'ils soient organisés au niveau de l'entité critique. Ces exercices couvrent les types de risques auxquels l'entité critique peut être confrontée et pour lesquels il est possible de mettre en place des exercices.

Art. 19

Le risque existe que les collaborateurs des entités critiques ou leurs contractants abusent par exemple de leurs droits d'accès pour causer des dommages au sein de l'organisation de l'entité critique. L'article 14 de la directive CER prévoit dès lors une possibilité de vérification des antécédents. Cette possibilité existe en Belgique sur base de l'article 27 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité, et au service public réglementé, L'article 19 précise que l'autorité sectorielle peut demander une vérification de sécurité soit effectuée conformément à la loi précitée. L'article 19 s'applique par conséquent sans préjudice de l'application de la loi du 11 décembre 1998. Ceci permet d'examiner si, pour une entité critique, des vérifications de sécurité doivent être effectuées pour le personnel concerné.

Cet article est sans préjudice des réglementations sectorielles qui existent déjà à ce sujet.

Art. 20

En vertu de cet article, l'entité critique a l'obligation de notifier les incidents qui sont de nature à perturber de manière importante la fourniture de services essentiels, pour que les autorités compétentes puissent réagir rapidement et adéquatement aux incidents et se faire une idée complète de l'impact, de la nature, de la cause et des conséquences possibles des incidents auxquels les entités critiques sont confrontées et, le cas échéant, prendre les mesures de protection externes les plus adéquates.

Deze verplichtingen doet geen afbreuk aan de informatie die verplicht gegeven moet worden aan andere autoriteiten of diensten in het raam van andere wettelijke of reglementaire bepalingen. Het is inderdaad mogelijk dat een bevoegde overheid op dat vlak van beveiliging in een bepaalde sector of deelsector wettelijk gezien verwittigd moet worden van een incident.

Het Nationaal Centraal Contactpunt moet overigens, indien een incident aanzienlijke gevolgen heeft of kan hebben voor kritieke entiteiten en voor de continuïteit van de verlening van essentiële diensten in één of meer lidstaten, het Nationaal Centraal Contactpunt van de betrokken lidstaten verwittigen.

HOOFDSTUK 6

Rapportage en informatie-uitwisseling

Afdeling 1

De bevoegde autoriteiten

Art. 21

De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit die de rol van deze nationale autoriteit moet vervullen, is het Nationaal Crisiscentrum. Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en door Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.

Deze autoriteit wordt tevens aangeduid als het Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de lidstaten van de Europese Unie. Het betreft de omzetting van artikel 9, tweede paragraaf, van de Richtlijn.

Paragraaf 2 geeft delegatie aan de Koning om de coordinerende rol van deze autoriteit verder uit te werken. Het kan gaan over de facilitering van informatie-uitwisseling tussen sectorale overheden onderling, gelet op de nadruk die de CER-Richtlijn legt op de intersectorale afhankelijkheden tussen kritieke entiteiten, alsook over de rol die deze autoriteit kan opnemen ter ondersteuning van de sectorale overheden.

Ces obligations ne portent pas préjudice aux informations qui doivent être obligatoirement fournies aux autres autorités ou services dans le cadre d'autres dispositions légales ou réglementaires. Il est en effet possible qu'une autorité compétente doive être avertie d'un incident sur le plan de la sécurité dans un secteur ou sous-secteur déterminé.

Si un incident a ou peut avoir un effet perturbateur important pour les entités critiques ou pour la continuité de la fourniture des services essentiels dans un ou plusieurs États membres, le Point de Contact Central National doit par ailleurs en avertir le Point de Contact Central National des États membres concernés.

CHAPITRE 6

Rapportage et échange d'informations

Section 1re

Les autorités compétentes

Art. 21

Le Roi désigne l'autorité qui, en tant qu'autorité nationale, est chargée de suivre et de coordonner l'application de la présente loi.

L'autorité envisagée pour remplir le rôle d'autorité nationale est le Centre de Crise National. Il n'est pas directement cité dans la loi car, comme a déjà pu le préciser la section de législation du Conseil d'État, notamment dans l'avis 63.296/4, désigner directement des services du pouvoir exécutif créés par le Roi et qui dépendent de Lui serait une immixtion du pouvoir législatif dans l'organisation interne du pouvoir exécutif.

Cette autorité est également désignée comme Point de Contact Central National pour la résilience des entités critiques, pour tous les secteurs et sous-secteurs, pour la Belgique dans ses relations avec la Commission européenne et les États membres de l'Union européenne. Il s'agit de la transposition de l'article 9, paragraphe 2, de la directive.

Le paragraphe 2 donne une délégation au Roi pour définir plus avant le rôle de coordination de cette autorité. Il peut s'agir de faciliter l'échange d'informations entre les autorités sectorielles, vu l'accent que la directive CER met sur les dépendances intersectorielles entre les entités critiques, et de préciser le rôle que cette autorité peut jouer afin de soutenir les autorités sectorielles.

De Koning wijst tevens de sectorale overheden aan die belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet, behalve wanneer de sectorale overheden zelf bij wet werden opgericht.

Art. 22

Artikel 4 van de CER-Richtlijn legt aan elke lidstaat op om een strategie vast te stellen om de weerbaarheid van kritieke entiteiten te verbeteren, welke moet zorgen voor een integrale aanpak betreffende de weerbaarheid van kritieke entiteiten. De strategie moet de uit te voeren strategische doelstellingen en beleidsmaatregelen bevatten. In het belang van samenhang en efficiëntie moet de strategie zo worden ontworpen dat het bestaande beleid er naadloos in wordt geïntegreerd, en dat waar mogelijk wordt voortgebouwd op bestaande nationale en sectorale strategieën, plannen of soortgelijke documenten.

De Koning wijst de autoriteit aan die verantwoordelijk is voor het opstellen van deze nationale strategie.

Afdeling 2

Informatie-uitwisseling

Art. 23

De informatie die vertrouwelijk is op grond van Unie- of nationale regelgeving, zoals voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie, wordt uitsluitend met de betrokken autoriteiten, overeenkomstig deze wet, uitgewisseld wanneer dat noodzakelijk is voor de toepassing van deze wet. Er wordt uitsluitend informatie gewisseld die relevant is voor en evenredig is met het doel van die uitwisseling.

Bij elke uitwisseling van informatie worden de vertrouwelijkheid van die informatie en de veiligheids- en commerciële belangen van kritieke entiteiten gewaarborgd.

Art. 24

Het NCCN kan in het kader van haar coördinerende opdracht het vrijwillig delen van informatie tussen kritieke entiteiten faciliteren. Dit artikel werd toegevoegd naar aanleiding van het advies van de Raad van State. (Adv. RvS nr. 76.573/2/V, 59.)

Le Roi désigne également les autorités sectorielles responsables du contrôle de l'application des dispositions de la présente loi, sauf lorsque les autorités sectorielles elles-mêmes ont été instituées par la loi.

Art. 22

L'article 4 de la directive CER impose à chaque État membre de définir une stratégie destinée à améliorer la résilience des entités critiques, qui doit garantir une approche intégrale en matière de résilience des entités critiques. La stratégie doit contenir les objectifs et les mesures stratégiques à mettre en œuvre. Dans un souci de cohérence et d'efficacité, la stratégie doit être conçue de façon à intégrer aisément la politique existante et se baser, dans la mesure du possible, sur les stratégies, plans ou documents similaires qui existent au niveau national et sectoriel.

Le Roi désigne l'autorité responsable de la rédaction de cette stratégie nationale.

Section 2

Échange d'informations

Art. 23

Les informations confidentielles en vertu des réglementations de l'Union ou des réglementations nationales, telles que les réglementations relatives à la confidentialité des informations commerciales, ne sont échangées avec les autorités compétentes, conformément à la présente loi, que lorsque cela est nécessaire aux fins de la présente loi. Seules les informations pertinentes et proportionnées à l'objectif de cet échange sont échangées.

Lors de tout échange d'informations, la confidentialité de ces informations ainsi que la sécurité et les intérêts commerciaux des entités critiques sont préservés.

Art. 24

Dans le cadre de sa mission de coordination, le NCCN peut faciliter le partage volontaire d'informations entre les entités critiques. Cet article a été ajouté suite à l'avis du Conseil d'État. (Avis C.E. n° 76.573/2/V, p. 59.)

Art. 25

Het NCCN, het OCAD en in voorkomend geval, het CCB, werken, elks vanuit hun eigen bevoegdheden, samen om de bescherming te verzekeren van de kritieke entiteiten op het Belgisch grondgebied.

Om deze opdracht te verwezenlijken moeten ze de nuttige informatie kunnen verzamelen om externe beschermingsmaatregelen te kunnen nemen.

Art. 26

Dit artikel voorziet in een algemeen samenwerkingsprincipe tussen de kritieke entiteiten en de bevoegde overheden voor de bescherming van kritieke entiteiten teneinde de interne weerbaarheidsmaatregelen en de externe beschermingsmaatregelen op elkaar af te stemmen en op die manier de weerbaarheid van de entiteiten te optimaliseren. De samenwerking met de bevoegde overheden gebeurt op basis van hun eigen opdracht en bevoegdheden.

Deze samenwerking vloeit voort uit artikel 10 van de CER-Richtlijn, dat aanzet tot het faciliteren van de informatie-uitwisseling over aangelegenheden die onder deze Richtlijn vallen.

De verwijzing naar het contactpunt van de kritieke entiteit werd toegevoegd ter volledigheid.

Art. 27

Artikel 27 verleent een delegatie aan de Koning om te bepalen, voor een bepaalde sector of deelsector, of de informatie in het W.P.E nuttig kan zijn voor de opdrachten van de verschillende diensten belast met de externe bescherming van de kritieke entiteiten, te weten het NCCN en het OCAD en zo ja, om deze informatie te bepalen en de nadere regels te omschrijven volgens dewelke deze overheden ertoe toegang kunnen krijgen.

Omdat de inhoud van het W.P.E. en de gevoeligheidsgraad van de informatie die het bevat sector per sector verschilt, kan dat niet geval per geval in de wet worden geregeld, maar moet dat per sector gebeuren.

Art. 28

Dit artikel voorziet de mogelijkheid dat het NCCN en de sectorale overheden de kritieke entiteit op de hoogte brengen van relevante informatie die een impact kan hebben op zijn weerbaarheid of op de externe

Art. 25

Le NCCN, l'OCAM et, le cas échéant, le CCB, coopèrent, chacun dans le cadre de ses compétences, en vue d'assurer la protection des entités critiques sur le territoire belge.

Afin de remplir cette mission, ils doivent pouvoir recueillir les informations utiles pour prendre des mesures de protection externes.

Art. 26

Le présent article prévoit un principe général de coopération entre les entités critiques et les autorités compétentes pour la protection des entités critiques en vue d'harmoniser les mesures de résilience internes et les mesures de protection externes et d'optimiser ainsi la résilience des entités. La coopération avec les autorités compétentes se fait sur la base de leurs mission et compétences respectifs.

Cette collaboration découle de l'article 10 de la directive CER, qui incite à faciliter l'échange d'informations sur des questions qui relèvent de cette directive.

La référence au point de contact de l'entité critique a été ajoutée par souci d'exhaustivité.

Art. 27

L'article 27 donne délégation au Roi afin de déterminer, pour un secteur ou sous-secteur déterminé, si les informations contenues dans le P.R.E. peuvent être utiles pour les missions des différents services chargés de la protection externe des entités critiques, à savoir le NCCN et l'OCAM, et, si tel est le cas, de définir ces informations et les modalités selon lesquelles ces autorités peuvent y avoir accès.

Étant donné que le contenu du P.R.E. et le degré de sensibilité des informations qu'il contient diffèrent secteur par secteur, ceci ne peut pas être réglé au cas par cas dans la loi, mais doit l'être secteur par secteur.

Art. 28

Cet article prévoit la possibilité pour le NCCN et les autorités sectorielles de notifier à l'entité critique des informations pertinentes susceptibles d'avoir un impact sur sa résilience ou sur les mesures de protection

beschermingsmaatregelen, indien blijkt dat die informatie nuttig zou kunnen zijn voor de aanpassing van de interne weerbaarheidsmaatregelen. Het NCCN dient de noodzaak van een dergelijke mededeling te beoordelen, wat geval per geval moet worden geëvalueerd, aangezien systematische communicatie niet kan worden overwogen gelet op de gevoeligheidsgraad die bepaalde informatie kan hebben. Het NCCN kan een kopie van deze informatie naar de betrokken sectorale overheid sturen teneinde deze op de hoogte te houden van eventuele dreigingen die wegen op haar sector.

De communicatie van dit soort informatie ligt in de lijn van de coördinatierol die het NCCN speelt inzake de weerbaarheid van kritieke entiteiten. Het gaat erom een mechanisme in te stellen voor de uitwisseling van informatie, waardoor coördinatie mogelijk moet zijn tussen de overheden en de kritieke entiteiten, en dat daardoor een zekere concordantie bestaat tussen de intern en extern genomen maatregelen.

Art. 29

Dit artikel voorziet in een beperkte verspreiding van de informatie betreffende de criteria en de drempelwaarden of de niveaus van weerslag van de criteria vastgelegd door de sectorale overheid, omdat die criteria of drempels gevoelige informatie kunnen onthullen over een bepaalde entiteit of infrastructuur, wat haar beveiliging en bescherming kan schaden. Dezelfde beperkte verspreiding is van toepassing op de informatie in het W.P.E. die ter kennis gebracht wordt van de sectorale overheid, van de inspectiedienst, en van het OCAD krachtens dit artikel.

De mogelijkheid om te voorzien in beperkte verspreiding vindt zijn rechtsgrond in artikel 20 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst, dat bepaalt: “De documenten waarvan de overheid van oorsprong de verspreiding wil beperken tot de personen die bevoegd zijn om er kennis van te nemen, zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet, worden gemerkt met de vermelding “Beperkte verspreiding””.

In het raam van dit ontwerp vormt de beperkte verspreiding het beschermingsniveau dat minimaal moet worden toegekend aan de betrokken informatie, onverminderd de mogelijkheid voor de bevoegde overheid om haar te classificeren overeenkomstig de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst. Het artikel 3 van deze

externes, s’il apparaît que ces informations pourraient être utiles pour l’adaptation des mesures de résilience internes. Le NCCN est tenu d’évaluer la nécessité d’une telle communication en procédant au cas par cas, étant donné qu’une communication systématique ne peut être envisagée vu le degré de sensibilité de certaines informations. Le NCCN peut envoyer une copie de ces informations à l’autorité sectorielle concernée afin de la tenir informée des menaces éventuelles qui pèsent sur son secteur.

La communication de ce type d’informations s’inscrit dans le rôle de coordination que le NCCN remplit en matière de résilience des entités critiques. Il s’agit d’instaurer un mécanisme d’échange d’informations qui devrait permettre une coordination entre les autorités et les entités critiques, et ainsi de garantir une certaine concordance entre les mesures prises en interne et en externe.

Art. 29

Cet article prévoit une diffusion limitée des informations relatives aux critères et aux valeurs seuils ou aux niveaux de répercussion des critères fixés par les autorités sectorielles, parce que ces critères ou seuils peuvent entraîner la divulgation d’informations sensibles concernant une entité ou infrastructure déterminée, ce qui peut nuire à sa sécurité et sa protection. Cette même diffusion limitée s’applique aux informations contenues dans le P.R.E. et qui sont portées à la connaissance des autorités sectorielles, du service d’inspection, et de l’OCAM en vertu du présent article.

La possibilité de prévoir une diffusion limitée trouve son fondement juridique dans l’article 20 de l’arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, qui stipule: “Les documents dont l’autorité d’origine veut limiter la diffusion aux personnes qualifiées pour en connaître sans attacher à cette limitation les effets juridiques prévus par la loi, sont revêtus de la mention “Diffusion restreinte””.

Dans le cadre du présent projet, la diffusion limitée constitue le niveau de protection qui doit au moins être accordé aux informations concernées, sans préjudice de la possibilité pour l’autorité compétente de les classer conformément à la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé. L’article 3 de cette loi stipule en effet “Peuvent faire l’objet d’une

wet bepaalt inderdaad dat “In een classificatie kunnen worden ondergebracht: informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, waarvan de niet-geëigende aanwending schade kan toebrengen aan een van de volgende belangen:

(…)

c) de inwendige veiligheid van de Staat, (…);

e) het wetenschappelijk en economisch potentieel van het land;

f) elk ander fundamenteel belang van de Staat;

(…)”.

Een dergelijke classificatie zal welteverstaan de noodzakelijkheid met zich meebrengen, voor de personen die kennis nodig hebben van deze informatie in de uitoefening van hun functies, houder te zijn van een veiligheidsmachtiging van een passend niveau, hetzij vertrouwelijk, geheim of zeer geheim volgens het classificatieniveau.

Art. 30

Dit artikel legt de kritieke entiteit de verplichting van het beroepsgeheim op voor alle informatie in het W.P.E., omdat daarin gevoelige informatie kan staan die, indien ze bekend zou worden, de weerbaarheid van de kritieke entiteit zou kunnen schaden.

Onverminderd artikel 27, dat voorziet in het recht voor het NCCN en voor het OCAD om, binnen de door de Koning bepaalde grenzen, toegang te krijgen tot informatie uit het W.P.E., mag dergelijke informatie enkel maar worden overgemaakt aan personen die deze nodig hebben in de uitoefening van hun functies of opdracht. Het gaat dan met name om personen die gemachtigd zijn om veiligheidskwesties te behandelen in het raam van het contactpunt van de kritieke entiteit, alsook van de sectorale overheid.

Hetzelfde geheim is van toepassing op de informatie waarvan sprake is in hoofdstuk 4 van het ontwerp van wet alsook op de informatie die aan de entiteit in kennis wordt gebracht met toepassing van Hoofdstuk 4, de artikelen 18, § 6, 20, 26 en 28.

Dit beroepsgeheim overtreden is onderhevig aan de straffen voorzien bij artikel 458 van het Strafwetboek.

classification: les informations, documents ou données, le matériel, les matériaux ou matières, sous quelque forme que ce soit, dont l’utilisation inappropriée peut porter atteinte à l’un des intérêts suivants:

(…)

c) la sûreté intérieure de l’État, (…);

e) le potentiel scientifique et économique du pays;

f) tout autre intérêt fondamental de l’État;

(…)”.

Une telle classification entraînera bien entendu la nécessité, pour les personnes qui ont besoin d’avoir connaissance de ces informations dans l’exercice de leurs fonctions, d’être détenteur d’une habilitation de sécurité d’un niveau approprié, soit confidentiel, secret ou très secret selon le niveau de classification.

Art. 30

Le présent article impose à l’entité critique l’obligation de secret professionnel pour toutes les informations contenues dans le P.R.E., étant donné que ce dernier peut contenir des informations sensibles qui, si elles venaient à être divulguées, pourraient porter préjudice à la résilience de l’entité critique.

Sans préjudice à l’article 27, qui prévoit le droit pour le NCCN et pour l’OCAM d’accéder aux informations du P.R.E., dans les limites fixées par le Roi, ces informations peuvent uniquement être transmises aux personnes qui en ont besoin dans l’exercice de leurs fonctions ou de leur mission. Il s’agit notamment de personnes qui sont autorisées à traiter les questions de sécurité dans le cadre du point de contact de l’entité critique, ainsi que de l’autorité sectorielle.

Le même secret s’applique aux informations dont il est question au chapitre 4 du projet de loi, ainsi qu’aux informations qui sont portées à la connaissance de l’entité en application du Chapitre 4, des articles 18, § 6, 20, 26 et 28.

La violation de ce secret professionnel est punie des peines prévues à l’article 458 du Code pénal.

Art. 31

Aangezien het gaat om een beperkte verspreiding of om een classificatie bedoeld door het artikel 29 van dit ontwerp, dient het doel van bescherming van belangen hiervoor uiteengezet logischerwijze te primeren op het principe van openbaarheid van bestuur.

Art. 32

De sectorale overheid komt, in het kader van haar taak als bevoegde autoriteit voor de kritieke entiteiten, mogelijks in contact met geclassificeerde informatie. Hiernaast betreft alle informatie omtrent de weerbaarheid van kritieke entiteiten steeds gevoelige informatie. Teneinde een zo vlot mogelijke informatie doorstroom te faciliteren, werd er gekozen om de verplichting op te leggen voor het personeel dat toegang heeft tot informatie betreffende de weerbaarheid van kritieke entiteiten, om ervoor te zorgen dat minstens één iemand van dit personeel over een veiligheidsmachtiging van het niveau GEHEIM beschikt, als bedoeld in Hoofdstuk III van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst. De veiligheidsmachtiging betreft informatie uit België, de EU en NAVO. Op deze manier wordt er een veiligheidscultuur gecreëerd in de sectorale overheden, en is er zekerheid dat wanneer er geclassificeerde informatie gedeeld moet worden met een welbepaalde sectorale overheid, dit ook mogelijk is in de praktijk.

Delegatie wordt gegeven aan de Koning om het gehele of een deel van het W.P.E. te classificeren. Dit volgt uit het feit dat men in het W.P.E. alle relevante informatie in acht moet nemen, waaronder mogelijk geclassificeerde informatie. Het betreft geen verplichting hiertoe, aangezien dit ook administratieve gevolgen met zich meebrengt. De Koning waakt erover dat de bevoegde personen binnen de kritieke entiteit te allen tijde toegang hebben tot hun volledige W.P.E. Dit houdt in dat, in het geval van classificatie, deze personen ook beschikken over een adequaat niveau van veiligheidsmachtiging.

De classificatie zal gebeuren op voordracht van de bevoegde minister voor de welbepaalde sector of deelsector, zoals bepaald in bijlage. In het geval het een sector betreft die betrekking heeft op de bevoegdheden van de gefedereerde entiteiten, dan is de bevoegde minister de federale minister die vertegenwoordigd wordt in de vastgestelde *sui generis* sectorale overheid. Bijkomend betreft het de classificatie op grond van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst, waarvoor de federale

Art. 31

Étant donné qu'il s'agit d'une diffusion limitée ou d'une classification prévue à l'article 29 du présent projet, l'objectif de protection des intérêts, tel qu'exposé ci-avant, doit en toute logique primer sur le principe de publicité de l'administration.

Art. 32

L'autorité sectorielle, dans le cadre de son rôle d'autorité compétente pour les entités critiques, peut entrer en contact avec des informations classifiées. En outre, toutes les informations relatives à la résilience des entités critiques concernent toujours des informations sensibles. Afin de faciliter au maximum la circulation des informations, il a été décidé d'imposer au personnel ayant accès aux informations relatives à la résilience des entités critiques l'obligation de veiller à ce qu'au moins une personne de ce personnel dispose d'une habilitation de sécurité de niveau SECRET, telle que visée au chapitre III de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité, et au service public réglementé. L'habilitation de sécurité concerne les informations provenant de la Belgique, de l'UE et de l'OTAN. De cette manière, une culture de la sécurité est créée au sein des autorités sectorielles, et il est garanti que lorsque des informations classifiées doivent être partagées avec une autorité sectorielle spécifique, ce partage est également possible dans la pratique.

Une délégation est donnée au Roi pour classifier tout ou partie du P.R.E. Ceci découle du fait que toutes les informations pertinentes dans le P.R.E. doivent être prises en compte, y compris les informations potentiellement classifiées. Il ne s'agit pas d'une obligation, car ceci a également des implications administratives. Le Roi veille à ce que les personnes autorisées au sein de l'entité critique aient à tout moment accès à l'intégralité de leur P.R.E. Cela implique qu'en cas de classification, ces personnes disposent également d'un niveau d'habilitation de sécurité adéquat.

La classification se fera sur proposition du ministre compétent pour le secteur ou le sous-secteur en question, tel que stipulé dans l'annexe. Dans le cas d'un secteur relevant des compétences des entités fédérées, le ministre compétent est le ministre fédéral représenté au sein de l'autorité sectorielle *sui generis* établi. En outre, il s'agit de la classification en vertu de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, pour laquelle le ministre fédéral de la Justice est compétent. Par conséquent, le ministre fédéral compétent

minister van Justitie bevoegd is. Bijgevolg zullen de federaal bevoegde minister van de desbetreffende sector of deelsector, alsook de federale minister bevoegd voor de wetgeving betreffende de classificatie van informatie verantwoordelijk zijn voor het voordragen van de uitvoeringsbesluiten hieromtrent.

HOOFDSTUK 7

Controle en sancties

Afdeling 1

Inspecties en audits

Art. 33

Artikel 33 organiseert de controle op de naleving van zijn verplichtingen door de kritieke entiteit. Per sector moet door de Koning een inspectiedienst worden aangeduid die voor deze controle instaat, op initiatief van de minister die bevoegd is voor de sector. In voorkomend geval, kan een inspectiedienst per deelsector worden aangewezen, naargelang zijn eigen bijzonderheden.

Art. 34

Dit artikel heeft betrekking op de toezichthoudende bevoegdheden van de voor het toezicht bevoegde autoriteiten en de eraan verbonden waarborgen om ervoor te zorgen dat de rechten van de geïnspecteerde personen worden gerespecteerd. Dit artikel werd toegevoegd naar aanleiding van het advies van de Raad van State. (Adv. RvS nr. 76.573/2/V, 61.) Deze autoriteiten beschikken over ruime bevoegdheden om grondige controles uit te voeren op de naleving van het wetsontwerp. Gezien de omvang van de bevoegdheden van deze autoriteiten verduidelijkt paragraaf 4 van dit artikel dat de middelen die de beëdigde leden van de voor het toezicht bevoegde autoriteiten gebruiken, passend en noodzakelijk moeten zijn voor het toezicht op de naleving van het wetsontwerp.

De voor het toezicht bevoegde autoriteiten mogen met name de identiteit opnemen van de personen die aanwezig zijn bij een controle en zonder voorafgaande verwittiging alle lokalen betreden die door de gecontroleerde entiteit worden gebruikt. In de praktijk kunnen de namen van de personen die zonder voorafgaande verwittiging mogen binnengaan, vooraf worden verstrekt om de voorspelbaarheid te verbeteren. Indien de lokalen bewoond zijn, mogen deze autoriteiten de lokalen alleen

du secteur ou du sous-secteur concerné, ainsi que le ministre fédéral responsable de la législation relative à la classification des informations, seront chargés de proposer les arrêtés d'exécution en la matière.

CHAPITRE 7

Contrôle et sanctions

Section 1re

Inspections et audits

Art. 33

L'article 33 organise le contrôle du respect de ses obligations par l'entité critique. Par secteur, le Roi désigne un service d'inspection qui se charge de ce contrôle, à l'initiative du ministre chargé du secteur. Le cas échéant, un service d'inspection peut être désigné par sous-secteur en fonction de ses particularités.

Art. 34

Cet article porte sur les pouvoirs en matière de contrôle des autorités compétentes pour le contrôle et les garde-fous y afférents afin de garantir le respect des droits des personnes inspectées. Cet article a été ajouté suite à l'avis du Conseil d'État. (Avis C.E. n° 76.573/2/V, p. 61.) Ces autorités disposent de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du projet de loi. Étant donné l'étendue des pouvoirs conférés à ces autorités, l'article précise, en son paragraphe 4, que les moyens mis en œuvre par les membres assermentés des autorités compétentes pour le contrôle doivent être appropriés et nécessaires au contrôle du respect du projet de loi.

Les autorités compétentes pour le contrôle peuvent notamment prendre l'identité des personnes présentes lors d'un contrôle et pénétrer sans avertissement préalable dans tous les locaux utilisés par l'entité contrôlée. En pratique, le nom des personnes pouvant pénétrer sans avertissement préalable peut être fourni à l'avance pour plus de prévisibilité. Lorsqu'il s'agit de locaux habités, ces autorités ne peuvent y pénétrer que moyennant l'autorisation préalable d'un juge d'instruction. Le

betreden mits vooraf een machtiging is uitgereikt door de onderzoeksrechter. Paragraaf 2 gaat nader in op de procedure en de informatie die aan de onderzoeksrechter moet worden verstrekt.

Voorts komen de na te leven regels aan bod in geval van een verhoor en met betrekking tot de gegevens die mogen worden geraadpleegd.

Er wordt delegatie gegeven aan de Koning om de nadere regels voor de controle te specifiëren. Deze nadere regels moeten onder andere de opdrachten van de inspectiedienst, de frequentie van de controles, de minimale voorwaarden waaraan de inspecteleden moeten voldoen en de punten waarop de controle dient te gebeuren of de rapportering die aan de sectorale overheid moet worden gedaan, betreffen.

Art. 35

Artikel 21.1, b) van de CER-Richtlijn legt de verplichting op dat de bevoegde autoriteiten over de bevoegdheden en middelen beschikken om audits uit te voeren of te gelasten met betrekking tot kritieke entiteiten. Er wordt delegatie gegeven aan de Koning om de nadere regels omtrent de audits vast te leggen, zodat rekening gehouden kan worden met de specificiteiten van elke sector.

Afdeling 2

Procedure van de sancties

Dit ontwerp biedt naast de mogelijkheid tot strafsancties, nu ook de mogelijkheid tot het opleggen van administratieve sancties. De KI-wet bevatte enkel strafsancties, maar in de praktijk bleek dat het eerder ging over formele inbreuken die niet leidden tot ernstige incidenten. Het doel van sancties te voorzien is om een drukkingsmiddel ter beschikking te hebben wanneer nodig. De toevoeging van administratieve sancties zorgt ervoor dat, wanneer de procureur des Konings beslist om geen strafrechtelijke vervolging in te stellen, de sectorale overheid alsnog een administratieve sanctie kan opleggen aan de overtreder. Verplichtingen hebben immers meer gewicht als de niet-naleving ervan kan leiden tot sancties.

De toevoeging van de mogelijkheid om administratieve sancties op te leggen zorgt tevens voor harmonisatie in de sanctionering van kritieke entiteiten tussen de verschillende sectoren en deelsectoren. Sommige sectoren of deelsectoren kunnen reeds op basis van sectorspecifieke wetgeving administratieve sancties opleggen, terwijl andere sectoren dergelijk kader missen

paragraphe 2 détermine la procédure et les éléments à fournir au juge d'instruction.

Il est précisé également les règles à respecter en cas d'audition et celles relatives aux données consultables.

Une délégation est donnée au Roi pour spécifier les modalités du contrôle. Ces modalités doivent, entre autres, porter sur les missions du service d'inspection, la fréquence des inspections, les conditions minimales à remplir par les membres de l'inspection et les points à inspecter, ou les rapports à faire à l'autorité sectorielle.

Art. 35

L'article 21.1, b) de la directive CER impose aux autorités compétentes de disposer des compétences et des moyens pour effectuer des audits concernant les entités critiques. Une délégation est donnée au Roi pour fixer les modalités des audits afin de tenir compte des spécificités de chaque secteur.

Section 2

Procédure de sanctions

Outre la possibilité de sanctions pénales, ce projet prévoit désormais la possibilité de sanctions administratives. La loi IC ne prévoyait que des sanctions pénales, mais dans la pratique, il s'est avéré qu'il s'agissait davantage d'infractions formelles qui n'entraînaient pas d'incidents graves. L'objectif des sanctions est de disposer d'un moyen de pression en cas de besoin. L'ajout de sanctions administratives garantit que si le procureur du Roi décide de ne pas engager de poursuites pénales, l'autorité sectorielle peut toujours imposer une sanction administrative à l'auteur de l'infraction. En effet, les obligations ont plus de poids si leur non-respect peut entraîner des sanctions.

L'ajout de la possibilité d'imposer des sanctions administratives garantit également l'harmonisation des sanctions à l'encontre des entités critiques dans les différents secteurs et sous-secteurs. Certains secteurs ou sous-secteurs peuvent déjà imposer des sanctions administratives sur la base d'une législation sectorielle, tandis que d'autres secteurs ne disposent pas d'un tel

en dit dus niet kunnen. Dit zorgt voor grote verschillen en een ongelijkheid van behandeling tussen de sectoren, zowel voor wat betreft de hoogte van de administratieve boetes als voor wat betreft de procedurele aspecten. Daarnaast zorgt de toevoeging ervan voor een duidelijkere samenhang met de NIS 2-Richtlijn. De entiteiten die als kritiek geïdentificeerd worden onder CER, zullen ook essentiële entiteiten zijn onder NIS 2. Het is niet onwaarschijnlijk dat een bepaalde inbreuk, zowel een inbreuk op de CER- als de NIS 2-regelgeving uitmaakt, waardoor het van belang is dat het sanctiemechanisme van beide kaders coherent is.

Het kader voor administratieve sancties in deze wet doet geen afbreuk aan de reeds bestaande regelgeving voor administratieve sancties in bepaalde sectoren of deelsectoren. Afdeling 4 is bedoeld voor sectoren of deelsectoren die niet kunnen terugvallen op sectorspecifieke regelgeving voor administratieve sancties.

Art. 36

Het artikel beschrijft de procedure voor de vaststelling van inbreuken op de wet, de uitvoeringsbesluiten ervan of de hieraan verbonden individuele administratieve beslissingen.

Een eerste remediëringstermijn wordt bepaald door middel van een formele ingebrekestelling. Deze wordt voorafgegaan door een gemotiveerde mededeling aan de kritieke entiteit, die de mogelijkheid heeft om opmerkingen te formuleren en kan vragen om te worden gehoord. Vervolgens stuurt de inspectiedienst de overtreder de ingebrekestelling, met een termijn waarbinnen de kritieke entiteit zich in regel moet stellen.

In afwijking van paragraaf 2 wordt dergelijke gemotiveerde mededeling niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd.

Art. 37

Bij een gebrek aan remediëring na een ingebrekestelling, wordt een proces-verbaal opgemaakt door de beëdigde personeelsleden van de inspectiedienst en wordt een kopie van het proces-verbaal overgemaakt aan de sectorale overheid. Het origineel van het proces-verbaal wordt overgemaakt aan de procureur des Konings.

cadre et ne peuvent donc pas le faire. Ceci crée des différences significatives et une inégalité de traitement entre les secteurs, tant en ce qui concerne le niveau des amendes administratives que les aspects procéduraux. En outre, l'ajout de cette disposition renforce la cohérence avec la directive NIS 2. Il n'est pas improbable qu'une infraction donnée constitue une infraction à la fois à la réglementation CER et à la réglementation NIS 2, d'où l'importance de la cohérence du mécanisme de sanction prévu par les deux cadres.

Le cadre des sanctions administratives dans cette loi est sans préjudice des réglementations déjà existantes pour les sanctions administratives dans certains secteurs ou sous-secteurs. La section 4 est destinée aux secteurs ou sous-secteurs qui ne peuvent pas s'appuyer sur des réglementations sectorielles spécifiques pour les sanctions administratives.

Art. 36

L'article décrit la procédure de constatation des violations de la loi, de ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes.

Un premier délai de remédiation est déterminé par une mise en demeure. Celle-ci est précédée d'une communication motivée adressée à l'entité critique, qui a la possibilité de présenter des observations et de demander à être entendue. Le service d'inspection envoie ensuite la mise en demeure au contrevenant, assortie d'un délai dans lequel l'entité critique doit se mettre en conformité.

Nonobstant le paragraphe 2, cet avis motivé n'est pas envoyé à l'avance à l'entité concernée dans des cas exceptionnels dûment justifiés où une action immédiate visant à prévenir un incident ou à y répondre serait autrement entravée.

Art. 37

En cas de non-remédiation après une mise en demeure, un procès-verbal est dressé par le personnel assermenté du service d'inspection et une copie du procès-verbal est remise à l'autorité sectorielle. L'original du procès-verbal est remis au procureur du Roi.

De wet kent bijzondere bewijskracht toe aan de materiële vaststellingen die het voorwerp uitmaken van dat proces-verbaal. Dit is gerechtvaardigd gezien de technische aard van deze vaststellingen, die het in de praktijk moeilijk maakt om sommige aspecten van de in de wet bedoelde inbreuken vast te stellen op een andere wijze dan door de beëdigde inspecteurs of experten. Bovendien worden de rechten van de beklaagde niet beperkt aangezien het mogelijk blijft om het tegenbewijs aan te leveren met alle bewijsmiddelen die de rechter zal beoordelen.

Art. 38

Het is niet mogelijk om zowel strafrechtelijke als administratieve sancties op te leggen aan een kritieke entiteit. Indien er een strafrechtelijke sanctie werd opgelegd, zal het opleggen van een administratieve sanctie niet meer mogelijk zijn.

Art. 39

Volgens dit artikel beschikt de procureur des Konings over een termijn van twee maanden te rekenen vanaf de ontvangst van het proces-verbaal om een strafrechtelijke vervolging in te stellen tegen de kritieke entiteit, die hierover binnen dezelfde termijn wordt ingelicht. De dag van ontvangst wordt geacht de derde dag te zijn die volgt op deze waarop de kopie van het procesverbaal aan de postdiensten overhandigd werd, tenzij de geadresseerde het tegendeel bewijst.

Er mag geen administratieve geldboete worden opgelegd voor het verstrijken van deze termijn of voor de beslissing van de procureur des Konings om niet te vervolgen.

Art. 40

Voor wat betreft de deelsector vervoer over water zal een inbreuk op deze wetgeving vaak gelijklopen aan een inbreuk op het Belgisch Scheepvaartwetboek en de ISPS-Code. Hiervoor is een volledig eigen systeem van administratieve sancties voorzien overeenkomstig de wet van 25 december 2016 tot instelling van administratieve geldboetes van toepassing in geval van inbreuken op de scheepvaartwetten. Procedureel is het niet opportuun om een ander systeem van administratieve boetes in te stellen voor deze deelsector.

La loi attribue une force probante particulière aux constatations matérielles qui font l'objet de ce procès-verbal. Cela se justifie par le caractère technique de ces constatations qui, en pratique, rendent difficile la constatation de certains aspects des infractions visées par la loi autrement que par des inspecteurs ou des experts assermentés. En outre, les droits de l'accusé ne sont pas limités, puisqu'il reste possible de prouver le contraire à l'aide de tout élément de preuve que le tribunal appréciera.

Art. 38

Il n'est pas possible d'imposer à la fois des sanctions pénales et administratives à une entité critique. Si une sanction pénale a été imposée, l'imposition d'une sanction administrative ne sera plus possible.

Art. 39

Selon cet article, le procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour engager des poursuites pénales à l'encontre de l'entité critique, qui est notifiée dans le même délai. Le jour de réception est réputé être le troisième jour suivant celui où la copie du procès-verbal a été remise aux services postaux, sauf preuve contraire apportée par le destinataire.

Aucune amende administrative ne peut être imposée avant l'expiration de ce délai ou avant la décision du procureur du Roi de ne pas poursuivre.

Art. 40

En ce qui concerne le sous-secteur du transport par voie d'eau, une infraction à cette législation sera souvent équivalente à une infraction au Code maritime belge et au Code ISPS. Pour ce faire, un système de sanctions administratives totalement distinct est prévu conformément à la loi du 25 décembre 2016 établissant les amendes administratives applicables en cas d'infraction à la législation sur la navigation. D'un point de vue procédural, il n'est pas opportun d'établir un autre système d'amendes administratives pour ce sous-secteur.

Afdeling 3

Strafrechtelijke sancties

Art. 41

Dit artikel bepaalt de strafsancties die van toepassing zijn op de kritieke entiteit bij het niet in acht nemen van de verplichtingen die worden opgelegd bij dit ontwerp en bij de uitvoeringsbesluiten ervan, evenals in geval van belemmering van de controles uitgevoerd door de inspectiediensten.

Het strafstelsel is gebaseerd op wat bepaald werd in de wet KI, en dus reeds sinds 2011 in voege is.

De afwezigheid van de weerbaarheidsmaatregelen, het niet uitvoeren ervan of het verzuim de overheden te informeren over elke gebeurtenis die de weerbaarheid van kritieke entiteiten kan treffen, kunnen gevolgen hebben voor de essentiële dienstverlening, hetgeen een zekere strengheid van bestraffing verantwoordt. Het gaat erom de kritieke entiteit te responsabiliseren voor de impact dat zijn entiteit, en bijhorende kritieke infrastructuur, kan hebben op de essentiële dienstverlening in het land.

Artikel 41, § 2, voorziet in strafrechtelijke sancties voor eenieder die opzettelijk de uitvoering van een inspectie door leden van de inspectiedienst verhindert of belemmert, weigert de inlichtingen te verstrekken die hem in verband met deze inspectie worden gevraagd, of opzettelijk onjuiste of onvolledige inlichtingen verstrekt. Het spreekt vanzelf dat deze bepaling niet aldus kan worden uitgelegd dat een persoon tegen wie een vervolging is ingesteld, kan worden bestraft omdat hij weigert mee te werken aan het vaststellen van zijn eigen schuld, aangezien het recht om niet tegen zichzelf te getuigen wordt gewaarborgd door artikel 14, lid 3, sub g, van het Internationaal Verdrag inzake burgerrechten en politieke rechten en door artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens. Bijgevolg is artikel 41, § 2, alleen ontvankelijk in gevallen waarin de verplichting om de gevraagde informatie te verstrekken waarschijnlijk niet zal leiden tot een schending van het zwijgrecht.

Afdeling 4

Administratieve sancties

Art. 42

Dit artikel vermeldt het principe en het bedrag van de administratieve sancties.

Section 3

Les sanctions pénales

Art. 41

Le présent article détermine les sanctions pénales qui s'appliquent à l'entité critique en cas de non-respect des obligations qui sont imposées par le présent projet et ses arrêtés d'exécution, ainsi qu'en cas d'obstacle aux contrôles effectués par les services d'inspection.

Le système pénal se base sur les dispositions de la loi IC et est donc déjà en vigueur depuis 2011.

L'absence de mesures de résilience, leur non-exécution ou le fait de ne pas informer les autorités de chaque événement susceptible de nuire à la résilience des entités critiques, peut avoir des répercussions sur les services essentiels, ce qui justifie une certaine sévérité de la sanction. Il s'agit de responsabiliser l'entité critique quant à l'impact qu'elle-même et son infrastructure critique peuvent avoir sur les services essentiels du pays.

L'article 41, § 2, prévoit des sanctions pénales pour quiconque empêche ou entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou communique sciemment des informations inexactes ou incomplètes. Il va de soi que cette disposition ne pourrait être interprétée comme impliquant qu'une personne pénalement accusée puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité puisque le droit de ne pas s'auto incriminer est garanti par l'article 14, paragraphe 3, g), du Pacte international relatif aux droits civils et politiques et par l'article 6 de la Convention européenne des droits de l'Homme. Ainsi, l'article 41, § 2, n'est admissible que dans les hypothèses dans lesquelles l'obligation de communiquer les informations demandées n'est pas susceptible d'entraîner une méconnaissance du droit au silence.

Section 4

Les sanctions administratives

Art. 42

Cet article énonce le principe et le montant des sanctions administratives.

Het niet naleven van de verplichtingen in deze wet kan ernstige gevolgen hebben voor de essentiële dienstverlening.

Dezelfde opmerking als bij artikel 41, § 2, is van toepassing, met betrekking tot het recht om zichzelf niet te incrimineren.

Art. 43

Dit artikel regelt de principes voor het bepalen van het bedrag van de administratieve sanctie, de in aanmerking te nemen omstandigheden, de situaties van herhaling en de situaties van samenloop van inbreuken. De straffen moeten proportioneel zijn ten opzichte van de ernst van de inbreuk. Bij het toetsen van deze proportionaliteit wordt in het bijzonder rekening gehouden met de zwaarte van de inbreuk, de wijze waarop in gelijkaardige zaken werd geoordeeld en de weerslag van de sanctie voor de betrokken entiteit.

Met het oog op de eerbiediging van de rechten van verdediging is bepaald dat de overtreder kan worden gehoord of zijn verweermiddelen schriftelijk kan indienen binnen een termijn van vijftien dagen.

Op advies van het College van Procureurs-Generaal werd de mogelijkheid tot uitstel toegevoegd aan de tekst, teneinde de tekst in overeenstemming te brengen met de artikelen 10 en 11 van de Grondwet.

Art. 44

Dit artikel bepaalt dat de beslissing ter kennis wordt gebracht van de overtreder.

Art. 45

Dit artikel bepaalt de voorwaarden waarin de beslissing uitvoerbaar wordt.

Art. 46

Uit dit artikel blijkt dat de verjaringstermijn voor administratieve geldboetes drie jaar bedraagt.

Le non-respect des obligations prévues par cette loi peut avoir de graves conséquences pour les services essentiels.

La même observation que pour l'article 41, § 2 s'applique, en ce qui concerne le droit de ne pas s'auto-incriminer.

Art. 43

Cet article réglemente les principes de détermination du montant de la sanction administrative, les circonstances à prendre en compte, les situations de répétition et les situations de concours d'infractions. Les sanctions doivent être proportionnelles à la gravité de l'infraction. Lors de l'évaluation de cette proportionnalité, il est notamment tenu compte de la gravité de l'infraction, de la manière dont des cas similaires ont été jugés et de l'impact de la sanction sur l'entité concernée.

Afin de respecter les droits de la défense, il est prévu que le contrevenant peut être entendu ou peut présenter sa défense par écrit dans un délai de quinze jours.

Sur le conseil du Collège des procureurs généraux, la possibilité de sursis a été ajoutée au texte pour le mettre en conformité avec les articles 10 et 11 de la Constitution.

Art. 44

Cet article précise que la décision sera notifiée à l'auteur de l'infraction.

Art. 45

Cet article définit les conditions dans lesquelles la décision devient exécutoire.

Art. 46

Cet article indique que le délai de prescription pour les amendes administratives est de trois ans.

HOOFDSTUK 8

Sector overheid

Art. 47

Het wetgevend kader betreffende de kritieke entiteiten, dat historisch gezien werd opgesteld voor, en enkel werd toegepast op, de privésector, is niet zo eenvoudig op volledig dezelfde manier toepasbaar op de sector overheid. De weerbaarheid van de overheidsinstellingen in België is uiteraard minstens even belangrijk als in de privésector, doch noodzaakt de specificiteit van deze sector eigenlijk een gespecialiseerd of aangepast kader.

In de eerste plaats bemoeilijkt dit de keuze voor een sectorale overheid aangezien de scheidingslijn met de kritieke entiteit in deze sector vervaagt. Het zou daarnaast ook niet werkbaar zijn om de ene overheidsdienst aan de andere normen en verplichtingen te laten opleggen en doen afdwingen, waardoor het onmogelijk is om een algemene sectorale overheid voor de gehele sector aan te duiden. Ten slotte is de situatie voor elke federale overheidsdienst verschillend, zodat het noodzakelijk is dat elke minister zelf de invulling van de verplichtingen uit de wet kan vastleggen. Het wordt daarom niet opportuun geacht om alles in de wet zelf vast te leggen. Bijgevolg zal delegatie aan de Koning gegeven worden zodat dit sectoraal, en meer bepaald, per bevoegde minister, geregeld kan worden. Het onderscheid tussen de sector overheid en andere sectoren moet daarbij benadrukt worden. Binnen de overheidssector zullen geen digitale of elektriciteitsinfrastructuur te identificeren zijn, daar deze onder hun eigen sector vallen. Met de bevoegde minister wordt bedoeld, de minister bevoegd voor een welbepaalde kritieke entiteit binnen de sector overheid.

Omwille van de bovenstaande bijzondere eigenschappen van de sector overheid en de uitdagingen die deze met zich meebrengen wordt voor deze sector een bijzonder kader opgericht, gebaseerd op de verplichtingen uit de CER-Richtlijn en aangepast aan de specificiteiten van de sector. Voor deze sector zal volledig de *ratio legis* van de CER-Richtlijn gevolgd worden.

Op deze manier voldoet België aan zijn verplichting om de CER-Richtlijn tijdig om te zetten in nationale regelgeving, rekening houdend met de verschillen die bestaan tussen de private en publieke sector.

CHAPITRE 8

Secteur des administrations publiques

Art. 47

Le cadre législatif sur les entités critiques, historiquement rédigé et appliqué uniquement au secteur privé, n'est pas si facilement applicable de la même manière au secteur public. La résilience des institutions publiques en Belgique est évidemment au moins aussi importante que dans le secteur privé, mais la spécificité de ce secteur nécessite en fait un cadre spécialisé ou adapté.

En premier lieu, ceci complique le choix d'une autorité sectorielle, car la ligne de démarcation avec l'entité critique dans ce secteur est floue. En outre, il ne serait pas envisageable qu'une administration impose et fasse respecter des normes et des obligations à une autre, ce qui rendrait impossible la désignation d'une autorité sectorielle générale pour l'ensemble du secteur. Enfin, la situation étant différente pour chaque service public fédéral, il est nécessaire que chaque ministre puisse définir l'interprétation des obligations prévues par la loi. Il n'est donc pas jugé opportun de tout fixer dans la loi elle-même. C'est la raison pour laquelle délégation sera donnée au Roi afin que ceci puisse être réglé sectoriellement, et plus précisément, par ministre compétent. Il convient ici de souligner la distinction entre le secteur des administrations publiques et les autres secteurs. Aucune infrastructure numérique ou électrique ne sera identifiable au sein du secteur des administrations publiques, car elles relèvent de leur propre secteur. Par ministre compétent, on entend le ministre responsable d'une entité critique bien définie au sein du secteur des administrations publiques.

En raison des caractéristiques particulières du secteur public et des défis qu'il pose, un cadre spécial sera établi pour ce secteur, basé sur les obligations de la directive CER et adapté à ses spécificités. La *ratio legis* de la directive CER sera intégralement respectée pour ce secteur.

De cette manière, la Belgique remplit son obligation de transposer la directive CER dans la réglementation nationale en temps voulu, en tenant compte des différences qui existent entre le secteur privé et le secteur public.

HOOFDSTUK 9

Diverse bepalingen

Art. 48 tot 74

Elke vermelding van het wetgevend kader uit de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur, alsook de verwijzing naar de term “kritieke infrastructuur” wordt aangepast naar de nieuwe term “kritieke entiteit” en het nieuwe wetgevend kader uit dit ontwerp.

De bepaling tot wijziging van de wet van 10 juli 2006 in artikel 63 strekt tot uitbreiding van de verplichting van de ondersteunende diensten om persoonsgegevens en informatie mee te delen waarover zij beschikken in het kader van hun wettelijke taken en die relevant zijn voor de doeleinden van de dreigingsanalyse bedoeld in artikel 8, § 2, van de wet betreffende de weerbaarheid van kritieke entiteiten. Tot op heden zijn de ondersteunende diensten namelijk enkel verplicht om relevante en beschikbare informatie die betrekking heeft op de dreigingen terrorisme en extremisme aan het OCAD over te maken, hetgeen problematisch is vanuit het oogpunt van de dreigingsanalyse in het kader van de kritieke entiteiten. Deze wijziging is noodzakelijk aangezien het OCAD sinds de KI-wet reeds belast werd met het opstellen van strategische dreigingsanalyses die niet alleen terroristische en extremistische dreigingen omvatten, maar elk type dreiging wanneer dat het OCAD dit relevant acht voor de sector of deelsector, zonder het OCAD hiervoor aangepaste wettelijke instrumenten ter beschikking gesteld kreeg.

HOOFDSTUK 10

Slotbepalingen

Art. 75

Er wordt een machtiging aan de Koning gegeven om de regels op vlak van de weerbaarheid van kritieke entiteiten uit te breiden naar andere sectoren voor dewelke in de toekomst de bescherming van hun weerbaarheid noodzakelijk zou blijken in het belang van de ene of de andere essentiële dienstverlening.

De maatregelen genomen door de Koning zullen het voorwerp uitmaken van een overleg in de Ministerraad.

CHAPITRE 9

Dispositions diverses

Art. 48 à 74

Toutes les références au cadre législatif de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, ainsi que la référence au terme “infrastructure critique” doivent être adaptées au nouveau terme “entité critique” et au nouveau cadre législatif du présent projet.

La disposition modificative de la loi du 10 juillet 2006 dans l’article 63 vise à étendre l’obligation des services d’appui de communiquer les données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s’avèrent pertinents en vue d’atteindre les finalités de l’analyse de la menace visée à l’article 8, § 2, de la loi relative à la résilience des entités critiques. En effet, jusqu’à présent, les services d’appui sont uniquement tenus de transmettre à l’OCAM les informations pertinentes et disponibles relatives aux menaces de terrorisme et d’extrémisme, ce qui est problématique du point de vue de l’analyse des menaces dans le cadre des entités critiques. Ce changement est nécessaire car, depuis la loi IC, l’OCAM a déjà été chargé de préparer des évaluations stratégiques de la menace couvrant non seulement les menaces terroristes et extrémistes, mais tout type de menace lorsque l’OCAM le juge pertinent pour le secteur ou le sous-secteur, sans fournir à l’OCAM les instruments juridiques appropriés pour le faire.

CHAPITRE 10

Dispositions finales

Art. 75

Une habilitation est donnée au Roi pour étendre les règles de résilience des entités critiques à d’autres secteurs pour lesquels la protection de leur résilience s’avèrerait nécessaire à l’avenir, dans l’intérêt de l’un ou de l’autre service essentiel.

Les mesures prises par le Roi feront l’objet d’une délibération en Conseil des ministres.

Art. 76

Gelet op het uitvoerige kader dat in deze wet vervat zit met betrekking tot de weerbaarheid van kritieke entiteiten, wordt de wet van 1 juli 2011 betreffende de bescherming en de beveiliging van kritieke infrastructuren opgeheven. Het huidige ontwerp bestendigt het wetgevend kader uit de KI-wet, en breidt het verder uit op basis van de verplichtingen uit de CER-Richtlijn.

Art. 77

Volgens de termijnen vervat in deze wet moeten de kritieke entiteiten tien maanden na de kennisgeving van aanduiding als kritieke entiteit de weerbaarheidsmaatregelen uit het W.P.E. implementeren. Deze aanduiding dient uiterlijk te gebeuren op 17 juli 2026. Teneinde rechtszekerheid en continuïteit te waarborgen met betrekking tot het statuut als exploitant van kritieke infrastructuur wordt in dit artikel een overgangsbepaling voorzien, waarin bepaald wordt dat alle exploitanten van kritieke infrastructuren die op grond van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren als zodanig werden geïdentificeerd, vanaf 17 juli 2026 van rechtswege beschouwd worden als kritieke entiteiten.

Deze entiteiten zullen echter tot 17 mei 2027 gehouden worden aan de verplichtingen waaraan zij moesten voldoen op grond van de artikelen 13, 13/1, 13/2 en 14 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur, zodat er geen leemte kan ontstaan tussen de opheffing van wet van 2011 en de inwerkingtreding van de verplichtingen voor kritieke entiteiten uit dit ontwerp, en zodat het huidige veiligheidsniveau kan worden behouden tijdens de overgangsperiode.

Art. 78

Een dreigingsanalyse houdt rekening met de huidige, te verwachten en toekomstige dreiging. Er is dus geen reden waarom de analyse herhaald zou moeten worden als er nieuwe wetgeving van kracht wordt. Analyses die minder dan 4 jaar geleden zijn uitgevoerd, blijven daarom geldig voor de rest van de tijd, tenzij er een nieuwe factor zou zijn die een nieuwe dreigingsanalyse vereist.

Art. 76

Vu le cadre détaillé prévu par la présente loi en ce qui concerne la résilience des entités critiques, la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est abrogée. Le projet actuel perpétue le cadre législatif de la loi IC et l'élargit sur base des obligations de la directive CER.

Art. 77

Selon les délais prévus dans la présente loi, les entités critiques doivent mettre en œuvre les mesures de résiliences du P.R.E. dix mois après la notification de leur désignation en tant qu'entité critique. Cette désignation doit avoir lieu au plus tard le 17 juillet 2026. Afin d'assurer la sécurité juridique et la continuité du statut d'opérateur d'infrastructure critique, cet article prévoit une disposition transitoire, stipulant que tous les opérateurs d'infrastructures critiques identifiés comme tels en vertu de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques sont réputés être des entités critiques de plein droit à partir du 17 juillet 2026.

Toutefois, ces entités seront tenues aux obligations qu'elles devaient remplir en vertu des articles 13, 13/1, 13/2 et 14 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques jusqu'au 17 mai 2027, de sorte qu'il ne peut y avoir de décalage entre l'abrogation de la loi de 2011 et l'entrée en vigueur des obligations pour les entités critiques en vertu du présent projet, et de manière à ce que puisse être maintenu le niveau de sécurité actuel pendant la période de transition.

Art. 78

Une analyse de la menace tient compte de la menace actuelle, prévisible et à venir. Il n'y a, par conséquent, pas de raison que l'analyse soit renouvelée lors de l'entrée en vigueur d'une nouvelle législation. Les analyses réalisées il y a moins de 4 ans restent donc valables et ce, pour le solde de temps restant, sauf en cas de nouvel élément nécessitant une nouvelle analyse de la menace.

Art. 79

Gelet op het verstrijken van de deadline voor de omzetting van de CER Richtlijn op 17 oktober 2024, zal de wet inwerkingtreden de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

De eerste minister,

Bart De Wever

De minister van Economie en Landbouw,

David Clarinval

De minister van Volksgezondheid,

Frank Vandenbroucke

De minister van Financiën,

Jan Jambon

De minister van Justitie, belast met de Noordzee,

Annelies Verlinden

De minister van Veiligheid en Binnenlandse Zaken,

Bernard Quintin

De minister van Mobiliteit,

Jean-Luc Crucke

De minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid,

Vanessa Matz

Art. 79

Compte tenu de l'expiration du délai de transposition de la directive CER le 17 octobre 2024, la loi entrera en vigueur le jour de sa publication au *Moniteur belge*.

Le premier ministre,

Bart De Wever

Le ministre de l'Économie et de l'Agriculture,

David Clarinval

Le ministre de la Santé publique,

Frank Vandenbroucke

Le ministre des Finances,

Jan Jambon

La ministre de la Justice, chargée de la Mer du Nord,

Annelies Verlinden

Le ministre de la Sécurité et de l'Intérieur,

Bernard Quintin

Le ministre de la Mobilité,

Jean-Luc Crucke

La ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique,

Vanessa Matz

De minister van Energie,

Mathieu Bihet

De minister van Middenstand, Zelfstandigen en Kmo's,

Eléonore Simonet

Le ministre de l'Énergie,

Mathieu Bihet

La ministre des Classes moyennes, des Indépendants et des PME,

Eléonore Simonet

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten

HOOFDSTUK 1 – Algemene bepalingen

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2. Deze wet voorziet in de omzetting van de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG van de Raad.

HOOFDSTUK 2 – Definities

Art. 3. Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° "OCAD": Coördinatieorgaan voor de dreigingsanalyse ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging;

2° "sectorale overheid": de bevoegde autoriteit, aangewezen in bijlage of door de Koning, bij besluit vastgesteld na overleg in de Ministerraad, voor de in Bijlage vermelde sectoren en deelsectoren;

3° "kritieke entiteit": een publieke of particuliere entiteit die behoort tot het toepassingsgebied uit bijlage I, en die overeenkomstig Hoofdstuk 4, Afdeling 1, is geïdentificeerd als behorende tot een van de categorieën die zijn vermeld in de Bijlage;

4° "weerbaarheid": het vermogen van een kritieke entiteit om een incident te voorkomen, zich ertegen te beschermen, erop te reageren, er weerstand aan te bieden, en het mitigeren, absorberen, verwerken en herstellen van een incident;

5° "incident": elke gebeurtenis die het verlenen van een essentiële dienst aanzienlijk kan verstoren of verstoort, ook wanneer de gebeurtenis gevolgen heeft voor de nationale systemen die de rechtsstaat waarborgen;

6° "kritieke infrastructuur": een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, of een onderdeel van een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, hetgeen noodzakelijk is voor de verlening van een essentiële dienst;

7° "essentiële dienst": een dienst die van cruciaal belang is voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu;

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi concernant la résilience des entités critiques

CHAPITRE 1ER – Dispositions générales

Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2. Cette loi transpose la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques et abrogeant la directive 2008/114/CE du Conseil.

CHAPITRE 2 – Définitions

Art. 3. Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par:

1° "OCAM": Organe de coordination pour l'analyse de la menace institué par la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° "autorité sectorielle": l'autorité compétente désignée à l'annexe de la présente loi ou par le Roi, par arrêté pris après avis du Conseil des ministres, pour les secteurs et sous-secteurs désignés dans la même Annexe;

3° "entité critique": une entité publique ou privée identifiée comme telle conformément au Chapitre 4, Section 1re, appartenant à l'une des catégories énumérées en Annexe;

4° "résilience": la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir;

5° "incident": un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit;

6° "infrastructure critique": un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel;

7° "service essentiel": un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement;

8° “risico”: de mogelijkheid van verlies of verstoring als gevolg van een incident, dat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

9° “risicobeoordeling”: het gehele proces ter bepaling van de aard en omvang van een risico door potentiële relevante dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden, in kaart te brengen en te analyseren, en door het verlies of de verstoring van een essentiële dienst die dat incident zou kunnen veroorzaken in te schatten;

10° “SICAD”: Communicatie- en informatiedienst van het arrondissement, zoals bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

11° “overheidsinstantie”: een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

1° zij hangt af van de Federale Staat;

2° zij is niet van industriële of commerciële aard;

3° zij oefent niet hoofdzakelijk een activiteit uit die tot een van de andere sectoren of deelsectoren uit de bijlage behoren;

4° zij is geen privaatrechtelijke rechtspersoon.

12° “NIS 2-wet”: de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

HOOFDSTUK 3 – Toepassingsgebied

Art. 4. § 1. Deze wet is van toepassing op de sectoren en deelsectoren zoals vermeld in Bijlage.

Deze wet is echter niet van toepassing op de nucleaire installaties bedoeld bij de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

Art. 5. § 1. De bepalingen van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en Hoofdstuk 7 van deze wet zijn niet van toepassing op de als kritiek geïdentificeerde entiteiten in de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuren, tenzij de Koning anders bepaalt om tot een hoger weerbaarheidsniveau van die kritieke entiteiten te komen.

§ 2. Wanneer specifieke wetgeving voor sectoren of deelsectoren vereist dat kritieke entiteiten maatregelen dienen te nemen om hun weerbaarheid te vergroten, kan de Koning

8° “risque”: le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l’ampleur de cette perte ou de cette perturbation et la probabilité que l’incident se produise;

9° “évaluation des risques”: l’ensemble du processus permettant de déterminer la nature et l’étendue d’un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d’un service essentiel causée par cet incident;

10° “SICAD”: Service d’information et de communication de l’arrondissement, tel que visé par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

11° “entité de l’administration publique”: une autorité administrative visée à l’article 14, § 1er, alinéa 1er, des lois coordonnées sur de Conseil d’État qui satisfait aux critères suivants:

1° elle dépend de l’État fédéral;

2° elle n’a pas de caractère industriel ou commercial;

3° elle n’exerce pas à titre principal une activité relevant de l’un des autres secteurs ou sous-secteurs de l’annexe;

4° elle n’est pas une personne morale de droit privé.

12° “loi NIS 2”: la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique.

CHAPITRE 3 – Champ d’application

Art. 4. Cette loi s’applique à tous les secteurs et sous-secteurs mentionnés à l’Annexe de la présente loi.

Cette loi ne s’applique toutefois pas aux installations nucléaires au sens de la loi du 15 avril 1994 relative à la protection de la population et de l’environnement contre les dangers résultant des rayonnements ionisants et relative à l’Agence Fédérale du Contrôle Nucléaire, à l’exception des éléments d’une installation nucléaire destinée à la production industrielle d’électricité qui servent au transport de l’électricité.

Art. 5. § 1er. Les dispositions du Chapitre 4, Section 2, du Chapitre 5 et du Chapitre 7 de la présente loi ne s’appliquent pas aux entités identifiées comme critiques dans les secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques, sauf si le Roi en décide autrement pour atteindre un niveau de résilience plus élevé de ces entités critiques.

§ 2. Lorsqu’une législation spécifique à des secteurs ou sous-secteurs impose aux entités critiques de prendre des mesures pour accroître leur résilience, le Roi peut déterminer

bepalen dat deze maatregelen als gelijkwaardig worden beschouwd aan de verplichtingen uit hoofde van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en Hoofdstuk 7 van deze wet. In dat geval zijn deze bepalingen niet van toepassing op deze sectoren of deelsectoren.

Art. 6. § 1. Deze wet is voor de sector overheid niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten en de algemene inspectie bedoeld in artikel 2, 2° en 3°van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° NCCN;

9° nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van NIS2-wet.

§ 2. Hoofdstuk 4, Afdeling 2, en Hoofdstukken 5 en 7 van deze wet zijn in elk geval niet van toepassing op kritieke entiteiten die geïdentificeerd werden op grond van Hoofdstuk 4, Afdeling 1, van deze wet, die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten, of die uitsluitend diensten verlenen aan de in paragraaf 1 bedoelde overheidsinstanties.

que ces mesures sont considérées comme équivalentes aux obligations prévues au Chapitre 4, Section 2, au Chapitre 5 et au Chapitre 7 de la présente loi. Dans ce cas, les présentes dispositions ne s'appliquent pas à ces secteurs ou sous-secteurs.

Art. 6. § 1er. Pour le secteur des administrations publiques, cette loi ne s'applique pas:

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au Ministère de la Défense visé à l'article 1er de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police et à l'inspection générale visés à l'article 2, 2°, et 3°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le Ministère public inclus;

6° au Service public fédéral Justice crée par l'arrêté royal du 23 mai 2001 portant création du Service public fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visés au 5°;

7° aux missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° au NCCN;

9° à l'Autorité nationale de cybersécurité visée à l'article 16 de la loi NIS2.

§ 2. En tout état de cause, le Chapitre 4, Section 2, et les Chapitres 5 et 7 de la présente loi ne s'appliquent pas aux entités critiques identifiées conformément au Chapitre 4, Section 1re de la présente loi, qui exercent des activités dans le domaine de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales, ou qui fournissent des services exclusivement aux autorités publiques visées au paragraphe 1er.

HOOFDSTUK 4 – Identificatieprocedure

Afdeling 1. Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructuren

Art. 7. § 1 De sectorale overheid stelt een lijst op van essentiële diensten van de in Bijlage genoemde sectoren en deelsectoren.

§ 2 De sectorale overheid voert uiterlijk op 17 januari 2026, een risicobeoordeling uit, gebruikmakend van de lijst bedoeld in paragraaf 1, en vervolgens telkens wanneer dat nodig is en ten minste om de vier jaar, teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuren overeenkomstig deze Afdeling te identificeren, en die kritieke entiteiten te assisteren bij het nemen van maatregelen uit hoofde van artikel 18.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

§ 3. In de risicobeoordeling wordt rekening gehouden met relevante natuurlijke en door de mens veroorzaakte risico's, met inbegrip van intersectorale of grensoverschrijdende risico's, ongevallen, natuurrampen, noodsituaties op het gebied van volksgezondheid, hybride dreigingen en andere vijandelijke dreigingen, waaronder terroristische misdrijven als bedoeld in Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad.

§ 4. Bij de uitvoering van de risicobeoordeling houdt de sectorale overheid, wanneer relevant voor haar sector of deelsector, ten minste rekening met het volgende:

1° de algemene risicobeoordeling die is uitgevoerd overeenkomstig artikel 6, lid 1 van Besluit 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming;

2° andere relevante risicobeoordelingen, uitgevoerd overeenkomstig de voorschriften van de relevante sectorspecifieke wetgeving van de Europese Unie, met inbegrip van Verordening (EU) 2019/941 van het Europees Parlement en de Raad van 5 juni 2019 betreffende risicoparaatheid in de elektriciteitssector en tot intrekking van Richtlijn 2005/89/EG, Verordening (EU) 2017/1938 van het Europees Parlement en de Raad van 25 oktober 2017 betreffende maatregelen tot veiligstelling van de gasleveringszekerheid en houdende intrekking van Verordening (EU) 994/2010, en de Richtlijnen 2007/60/EG van het Europees Parlement en de Raad van 23 oktober 2007 over beoordeling en beheer van overstromingsrisico's en 2012/18/EU van het Europees Parlement en de Raad van 4 juli 2012 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken, houdende wijziging en vervolgens intrekking van Richtlijn 96/82/EG van de Raad;

CHAPITRE 4 – Procédure d'identification

Section 1re. Identification et désignation des entités critiques et des infrastructures critiques

Art. 7. § 1er L'autorité sectorielle prépare une liste de services essentiels des secteurs et sous-secteurs énumérés en Annexe.

§ 2. L'autorité sectorielle procède, à l'aide de la liste visée au paragraphe 1er, à une évaluation des risques au plus tard le 17 janvier 2026, et par la suite chaque fois que nécessaire et au moins tous les quatre ans, en vue d'identifier les entités critiques et leurs infrastructures critiques respectives conformément à la présente Section, et afin d'assister ces entités critiques à prendre des mesures en vertu de l'article 18.

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées, pour les entités critiques potentielles relevant de leurs compétences pour d'autres aspects.

§ 3. L'évaluation de risques tient compte des risques naturels et d'origine humaine pertinents, en ce compris les risques intersectoriels ou transfrontaliers, les accidents, les catastrophes naturelles, les urgences en matière de santé publique, les menaces hybrides et les autres menaces à caractère hostile, notamment les infractions terroristes visées par la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.

§ 4. Lors de l'évaluation des risques, l'autorité sectorielle prend au moins en compte les éléments suivants, lorsque cela est pertinent pour son secteur ou sous-secteur:

1° l'évaluation des risques effectuée conformément à l'article 6, paragraphe 1er, de la décision. 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union;

2° d'autres évaluations de risques pertinentes réalisées conformément aux exigences de la législation pertinente de l'Union européenne, notamment le règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin relatif à la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE, le règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz et abrogeant le règlement (UE) 994/2010, et les directives 2007/60/CE du Parlement européen et du Conseil du 23 octobre 2007 relative à l'évaluation et la gestion des risques d'inondation et 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des danger liés aux accidents majeurs impliquant des substances dangereuses, modifiant puis abrogeant la directive 96/82/CE du Conseil;

3° de relevante risico's die voortvloeien uit de afhankelijkheden tussen de in de Bijlage bedoelde sectoren, met inbegrip van de afhankelijkheid van in andere lidstaten en derde landen gevestigde entiteiten en de gevolgen die een significante verstoring in één sector kan hebben voor andere sectoren, met inbegrip van significante risico's voor de burgers en de interne markt;

4° alle informatie over incidenten waarvan op grond van artikel 20, paragraaf 1 is kennisgegeven.

Art. 8. § 1. Binnen een termijn van negen maanden, te rekenen vanaf de inwerkingtreding van deze wet, voert het OCAD een dreigingsanalyse uit voor de sectoren of deelsectoren vermeld in de Bijlage.

Deze dreigingsanalyse blijft gedurende maximaal vier jaar geldig vanaf de datum van voltooiing zoals aangegeven in artikel 77. Deze analyse wordt telkens wanneer nodig en ten minste één keer om de vier jaar vernieuwd.

Elke dreigingsanalyse die binnen vier jaar wordt uitgevoerd op basis van andere wetgeving voor de in Bijlage vermelde (deel-)sectoren moet voldoen aan de verplichtingen van dit artikel.

§ 2. De dreigingsanalyse in de zin van dit hoofdstuk bestaat uit een strategische gemeenschappelijke evaluatie zoals bedoeld in artikel 8, eerste lid, 1° van de wet van 10 juli 2006 betreffende de dreigingsanalyse.

De dreigingsanalyse heeft betrekking op elk type van dreiging die door het OCAD pertinent worden geacht ten aanzien van de sector of deelsector, die vallen onder de bevoegdheid van de ondersteunende diensten opgesomd in artikel 2, 2° van voornoemde wet van 10 juli 2006.

§ 3. De autoriteit bedoeld in artikel 21, § 1, de sectorale overheden en de ondersteunende diensten van het OCAD delen de informatiegegevens die nuttig zijn voor de uitvoering van de dreigingsanalyse bedoeld in paragraaf 1 mee aan het OCAD.

§ 4. Onverminderd artikel 10, § 1 van de voornoemde wet van 10 juli 2006 en artikel 8 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, wordt deze evaluatie meegedeeld aan de sectorale overheden zodat zij de conclusies van deze dreigingsanalyse kunnen opnemen in de risicoanalyse die zij krachtens artikel 7 moeten uitvoeren.

Art. 9. § 1. 1° Teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuren die onder haar bevoegdheid vallen te identificeren, overlegt de sectorale overheid vooraf met de autoriteit bedoeld in artikel 21, § 1, en raadpleegt zij de potentiële kritieke entiteiten en desgevallend de vertegenwoordigers van de sector.

De potentiële kritieke entiteiten zijn gehouden tot een degelijke informatie-uitwisseling met de sectorale overheid tijdens het identificatieproces.

3° les risques pertinents découlant des dépendances entre les secteurs visés en Annexe, y compris les dépendances à l'égard d'entités établies dans d'autres États membres et dans des pays tiers, et l'impact qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris les risques importants pour les citoyens et le marché intérieur;

4° toute information sur les incidents notifiés en vertu de l'article 20, paragraphe 1er.

Art. 8. § 1er. Dans un délai de neuf mois à compter de l'entrée en vigueur de la présente loi, l'OCAM procède à une analyse de la menace pour les secteurs ou sous-secteurs énumérés en Annexe.

Cette analyse de la menace reste valable pour un maximum de quatre ans à compter de sa réalisation comme prévu à l'article 77. Cette analyse est renouvelée chaque fois que nécessaire et au moins une fois tous les quatre ans.

Toute analyse de la menace réalisée endéans les quatre ans sur base d'une autre législation pour les (sous)-secteurs énumérés en Annexe doit être conforme aux obligations du présent article.

§ 2. L'analyse de la menace au sens du présent chapitre consiste en une évaluation stratégique commune telle que visée à l'article 8, alinéa 1er, 1° de la loi du 10 juillet 2006 relative à l'analyse de la menace.

L'analyse de la menace vise tout type de menace jugée pertinente par l'OCAM en ce qui concerne le secteur ou le sous-secteur, qui relèvent de la compétence des services d'appui, énumérés à l'article 2, 2° de la loi du 10 juillet 2006 susmentionnée.

§ 3. L'autorité visée à l'article 21, § 1er, les autorités sectorielles et les services d'appui de l'OCAM communiquent à l'OCAM les informations utiles pour effectuer l'analyse de la menace visée au paragraphe 1er.

§ 4. Sans préjudice de l'article 10, § 1er de la loi du 10 juillet 2006 susmentionnée et de l'article 8 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé, cette évaluation est communiquée aux autorités sectorielles afin de leur permettre d'intégrer les conclusions de cette analyse de la menace dans l'analyse de risques qu'elles sont tenues d'effectuer en vertu de l'article 7.

Art. 9. § 1er. 1° Afin d'identifier les entités critiques et leurs infrastructures critiques respectives relevant de sa compétence, l'autorité sectorielle consulte au préalable l'autorité visée à l'article 21, § 1er, les entités critiques potentielles et, le cas échéant, les représentants du secteur.

Les entités critiques potentielles sont tenues à des échanges d'informations appropriés avec l'autorité sectorielle au cours du processus d'identification.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

2° De sectorale overheid past de criteria, zoals bedoeld in artikel 10, § 1, toe teneinde een selectie te maken tussen de entiteiten die in haar sector bestaan en stelt een lijst op van de aldus geïdentificeerde potentiële kritieke entiteiten.

3° Of een incident een aanzienlijk verstorend effect heeft wordt bepaald in functie van de karakteristieken van de betrokken sector, op basis van de criteria bedoeld in artikel 10, § 2.

4° De sectorale overheid kan, in voorkomend geval, de sectorale criteria bedoeld in artikel 11 toepassen op deze lijst.

§ 2. De potentiële kritieke entiteit bezorgt aan de sectorale overheid binnen zes maanden na de raadpleging zoals bedoeld in de eerste paragraaf, een gemotiveerde lijst op van de bijhorende kritieke infrastructuren die noodzakelijk zijn voor de verlening van essentiële diensten. Deze lijst wordt gevalideerd door de bevoegde sectorale overheid, rekening houdende met de criteria uit artikel 10, paragraaf 2.

De sectorale overheid behoudt zich het recht voor om deze lijst te wijzigen, met opgave van motivatie hiervoor.

De kritieke entiteit is ten allen tijde verantwoordelijk voor het actualiseren van deze lijst, en stelt binnen 30 dagen na de wijziging de bevoegde sectorale overheid daarvan op de hoogte, met opgave van motivatie hiervoor. Elke wijziging dient gevalideerd te worden door de sectorale overheid. De sectorale overheid stelt op zijn beurt de autoriteit bedoeld in artikel 21, § 1, in kennis van deze wijziging.

De sectorale overheid waakt over de coherentie in haar sector of deelsector voor wat betreft de identificatie van kritieke infrastructuren.

§ 3. De Koning kan de voorwaarden en modaliteiten bepalen voor de informatie uitwisseling in het kader van de identificatieprocedure.

§ 4. Tijdens het identificatieproces als bedoeld in deze Afdeling wordt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de wet tot vaststellen van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hierna: NIS 2-Wet), betrokken bij het door de sectorale overheden en de autoriteit bedoeld in artikel 21, § 1, gevoerde overleg voor de identificatie van de kritieke entiteiten met betrekking tot de cyberbeveiliging van netwerk- en informatiesystemen.

Art. 10. § 1. De sectorale overheid houdt bij de identificatie van kritieke entiteiten overeenkomstig deze Afdeling rekening met de resultaten van de risicobeoordeling uit hoofde van artikel 7, en past alle volgende criteria toe:

1° de entiteit verleent één of meer essentiële diensten;

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées pour les entités critiques potentielles relevant pour d'autres aspects de leurs compétences.

2° L'autorité sectorielle applique les critères, tels que visés à l'article 10, § 1er, afin d'effectuer une sélection parmi les entités existantes dans son secteur, et établit une liste des entités critiques potentielles ainsi identifiées.

3° L'importance de l'effet perturbateur d'un incident est déterminée en fonction des caractéristiques du secteur concerné, sur la base des critères visés à l'article 10, § 2.

4° L'autorité sectorielle peut, le cas échéant, appliquer les critères sectoriels visés à l'article 11 à cette liste.

§ 2. L'entité critique potentielle transmet à l'autorité sectorielle, dans un délai de six mois à compter de la consultation visée au premier paragraphe, une liste motivée des infrastructures critiques qui y sont associées et qui sont nécessaires à la fourniture des services essentiels. Cette liste est validée par l'autorité sectorielle compétente, en tenant compte des critères énoncés à l'article 10, paragraphe 2.

L'autorité sectorielle se réserve le droit de modifier cette liste, en motivant sa décision.

L'entité critique est en tout temps responsable de la mise à jour de cette liste et notifie l'autorité sectorielle compétente endéans les 30 jours de la modification, en motivant sa décision. Toute modification doit être validée par l'autorité sectorielle. L'autorité sectorielle notifie à son tour cette modification à l'autorité visée à l'article 21, § 1er.

L'autorité sectorielle assure la cohérence dans son secteur ou sous-secteur en ce qui concerne l'identification des infrastructures critiques.

§ 3. Le Roi peut déterminer les conditions et les modalités concernant l'échange d'informations dans le cadre de la procédure d'identification.

§ 4. Lors du processus d'identification visé à la présente Section, l'autorité nationale de cybersécurité visée à l'article 16 de la loi du établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après: loi NIS 2) est associée aux consultations menées par les autorités sectorielles et l'autorité visée à l'article 21, § 1er, pour l'identification des entités critiques en ce qui concerne la cybersécurité des réseaux et des systèmes d'information.

Art. 10. § 1er. Lors de l'identification d'entités critiques conformément à la présente Section, l'autorité sectorielle tient compte des résultats de l'évaluation de risques prévue à l'article 7, et applique tous les critères suivants:

1° l'entité fournit un ou plusieurs services essentiels;

2° de entiteit is actief en haar kritieke infrastructuur bevindt zich op het Belgisch grondgebied;

3° een incident zou een aanzienlijk verstorend effect hebben op de verlening van deze essentiële diensten of andere essentiële diensten van de sectoren die onder het toepassingsgebied vallen van deze wet, zoals bepaald in de Bijlage.

§ 2. De sectorale overheid bepaalt, in overleg met de autoriteit bedoeld in artikel 21, § 1, en in voorkomend geval, na raapleging van de betrokken gefedereerde entiteiten, of een incident een aanzienlijk verstorend effect kan hebben op de verlening van essentiële diensten, rekening houdend met de volgende criteria:

1° het belang van de entiteit om de essentiële dienst op een voldoende niveau te houden, rekening houdend met de beschikbare alternatieven voor het verlenen ervan;

2° het aantal gebruikers dat afhankelijk is van de door de entiteit verleende essentiële dienst;

3° het marktaandeel van de entiteit op de markt voor dergelijke diensten;

4° de mate waarin andere in Bijlage genoemde sectoren afhankelijk zijn van die essentiële dienst;

5° de ernst en duur van de gevolgen die incidenten kunnen hebben voor de economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging en volksgezondheid;

6° het geografische gebied dat door een incident kan worden getroffen, met inbegrip van eventuele grensoverschrijdende gevolgen.

In het geconsolideerd dossier, zoals bedoeld in artikel 12, § 1, onderbouwt de sectorale overheid deze criteria op kwantitatieve en sectorspecifieke of deel-sectorspecifieke wijze, voor zover deze gegevens beschikbaar zijn. De autoriteit bedoeld in artikel 21, § 1, kan hierover gemotiveerd relevante informatie opvragen aan de sectorale overheid.

Art. 11. De sectorale overheid kan sectorale criteria bepalen waaraan de kritieke entiteiten moeten voldoen, rekening houdend met de bijzondere eigenschappen van de betrokken sector, in overleg met de autoriteit bedoeld in artikel 21, § 1, en, in voorkomend geval, na raadpleging van de betrokken gefedereerde entiteiten.

Art. 12. § 1. De sectorale overheid stelt een geconsolideerd dossier op, bestaande uit de volgende informatie:

1° een lijst van de geïdentificeerde potentiële kritieke entiteiten;

2° een lijst van de geïdentificeerde potentiële kritieke infrastructuren;

3° in voorkomend geval, de gebruikte sectorale criteria;

2° l'entité exerce ses activités sur le territoire belge et son infrastructure critique sont situées sur ledit territoire;

3° un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels ou d'autres services essentiels des secteurs relevant du champ d'application de la présente loi, tels que définis en Annexe.

§ 2. L'autorité sectorielle, en concertation avec l'autorité visée à l'article 21, § 1er, et, le cas échéant, après consultation des entités fédérées concernées, détermine si un incident pourrait avoir un effet perturbateur important sur la fourniture des services essentiels, en tenant compte des critères suivants:

1° l'intérêt de l'entité à maintenir un niveau adéquat de fourniture de service essentiel, en tenant compte des alternatives disponibles pour sa fourniture;

2° le nombre d'utilisateurs dépendant du service essentiel fourni par l'entité;

3° la part de marché de l'entité sur le marché de ces services;

4° la mesure dans laquelle d'autres secteurs énumérés en Annexe dépendent de ce service essentiel;

5° la gravité et la durée de l'impact que les incidents peuvent avoir sur les activités économiques et sociales, l'environnement, la sûreté et la sécurité publiques et la santé publique;

6° la zone géographique susceptible d'être affectée par un incident, y compris d'éventuels impacts transfrontaliers.

Dans le dossier consolidé, visé à l'article 12, § 1er, l'autorité sectorielle justifie ces critères de manière quantitative et de manière spécifique au secteur ou sous-secteur, lorsque ces données sont disponibles. L'autorité visée à l'article 21, § 1er, peut demander des informations pertinentes à ce sujet à l'autorité sectorielle, au moyen d'une demande motivée.

Art. 11. L'autorité sectorielle peut déterminer des critères sectoriels auxquels doivent répondre les entités critiques en tenant compte des particularités du secteur concerné, en concertation avec l'autorité visée à l'article 21, § 1er, et, le cas échéant, après avoir consulté les entités fédérées.

Art. 12. § 1er. L'autorité sectorielle prépare un dossier consolidé composé des informations suivantes:

1° une liste des entités critiques potentiellement identifiées;

2° une liste des infrastructures critiques potentiellement identifiées;

3° le cas échéant, les critères sectoriels utilisés;

4° de gebruikte criteria zoals bedoeld in artikel 10, § 2;

5° een uiteenzetting van de redenen.

De sectorale overheid zendt het geconsolideerd dossier ter advies over aan de autoriteit bedoeld in artikel 21, § 1, en, in voorkomend geval, ter informatie aan de betrokken gefedereerde entiteiten.

Nadat de sectorale overheid het advies bedoeld in het tweede lid ontvangen heeft, duidt zij de kritieke entiteiten en de respectievelijke kritieke infrastructuren aan, in voorkomend geval, na raadpleging van de betrokken gefedereerde entiteiten.

De autoriteit bedoeld in artikel 21, § 1, geeft bij elke substantiële wijziging in het geconsolideerde dossier opnieuw advies over die wijziging.

§ 2. Indien geen kritieke entiteit gelegen op het Belgisch grondgebied geïdentificeerd werd binnen een sector of deelsector, zet de bevoegde sectorale overheid, in een schrijven ter attentie van de autoriteit bedoeld in artikel 21, § 1, de redenen uiteen die geleid hebben tot deze afwezigheid van identificatie.

§ 3. De sectorale overheid duidt uiterlijk op 17 juli 2026 de kritieke entiteiten aan. De sectorale overheid voert het identificatieproces zoals beschreven in deze Afdeling minstens één keer om de vier jaar uit, voor wat betreft de kritieke entiteiten die tot haar sector behoren.

Art. 13. § 1. De sectorale overheid betekent, aan de entiteit, de met redenen omklede beslissing tot de aanduiding ervan als kritieke entiteit, met inbegrip van de kritieke infrastructuur, binnen een maand na de aanduiding als bedoeld in artikel 12. De sectorale overheid bezorgt aan de autoriteit bedoeld in artikel 21, § 1, een kopie van deze beslissing met de vermelding van de datum van betekening aan de desbetreffende kritieke entiteit.

§ 2. De autoriteit bedoeld in artikel 21, § 1, brengt op de hoogte van deze aanduiding:

1. de burgemeester van de gemeente op het grondgebied waarvan de kritieke infrastructuur van de kritieke entiteit zich bevindt;

2. de gouverneur van de provincie op het grondgebied waarvan de kritieke entiteit of haar kritieke infrastructuur zich bevindt of, wanneer de kritieke entiteit zich op het grondgebied van de Brusselse agglomeratie bevindt, de bevoegde overheid krachtens artikel 48 van de bijzondere wet van 12 januari 1989 met betrekking tot de Brusselse instellingen.

§ 3. De autoriteit bedoeld in artikel 21, § 1, bezorgt na de aanduiding van een kritieke entiteit en zijn respectievelijke kritieke infrastructuur, en daarna minstens jaarlijks, aan de door de Koning aangewezen dienst de gemeente waarin de kritieke infrastructuur zich bevindt of, in voorkomend geval, een lijst van de gemeenten waarin de kritieke infrastructuren zich bevinden voor de toepassing van artikel 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

4° les critères utilisés tels que visés à l'article 10, § 2;

5° une justification motivée.

L'autorité sectorielle envoie le dossier consolidé pour avis à l'autorité visée à l'article 21, § 1er et, le cas échéant, pour information aux entités fédérées.

Après avoir reçu l'avis visé au deuxième alinéa, l'autorité sectorielle désigne les entités critiques et les infrastructures critiques respectives et, le cas échéant, après consultation des entités fédérées.

Chaque fois qu'il y a un changement substantiel, l'autorité visée à l'article 21, § 1er, émet un nouvel avis sur toute modification substantielle du dossier consolidé.

§ 2. Si aucune entité critique située sur le territoire belge n'a été identifiée dans un secteur ou sous-secteur, l'autorité sectorielle compétente expose, dans un écrit à l'attention de l'autorité visée à l'article 21, § 1er, les raisons qui ont conduit à cette absence d'identification.

§ 3. L'autorité sectorielle désigne les entités critiques au plus tard le 17 juillet 2026. L'autorité sectorielle renouvelle le processus d'identification tel que décrit dans cette Section au moins une fois tous les quatre ans en ce qui concerne les entités critiques appartenant à son secteur.

Art. 13. § 1er. L'autorité sectorielle notifie à l'entité, dans un délai d'un mois après la désignation visée à l'article 12, la décision motivée de la désigner comme entité critique, y compris l'infrastructure critique. L'autorité sectorielle fournit à l'autorité visée à l'article 21, § 1er, une copie de cette décision avec mention de la date de la notification à l'entité critique concernée.

§ 2. L'autorité visée à l'article 21, § 1er, doit informer de cette désignation:

1. le bourgmestre de la commune sur le territoire de laquelle se trouvent les infrastructures critiques de l'entité critique;

2. le gouverneur de la province sur le territoire de laquelle l'entité critique ou son infrastructure critique se situe ou, lorsque l'entité critique se situe sur le territoire de l'agglomération bruxelloise, l'autorité compétente en vertu de l'article 48 de la loi spéciale du 12 janvier 1989 sur les institutions bruxelloises.

§ 3. Après la désignation d'une entité critique et de son infrastructure critique respective, et au moins une fois par an par la suite, l'autorité visée à l'article 21, § 1er, communique au service désigné par le Roi la commune dans laquelle l'infrastructure critique se situé ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées aux fins de l'article 126/3 de la loi du 13 juin 2005 relative aux communications électroniques.

§ 4. De autoriteit bedoeld in artikel 21, § 1, brengt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-wet op de hoogte van de aanduiding van de kritieke entiteiten.

Afdeling 2. Kritieke entiteiten van bijzonder Europees belang

Art. 14. § 1. Een entiteit wordt als een kritieke entiteit van bijzonder Europees belang beschouwd wanneer zij overeenkomstig artikel 12 als kritieke entiteit werd aangeduid, essentiële diensten verleent aan of in meer dan 6 lidstaten, en op grond van artikel 13, § 1 in kennis gesteld werd van haar aanduiding als kritieke entiteit.

§ 2. Na de kennisgeving van haar aanduiding overeenkomstig artikel 13, § 1, dient de kritieke entiteit de bevoegde sectorale overheid te informeren wanneer zij essentiële diensten verleent aan of in meer dan 6 lidstaten, welke essentiële diensten zij levert aan of in die lidstaten en aan of in welke lidstaten zij die essentiële diensten verleent.

De sectorale overheid stelt de autoriteit bedoeld in artikel 21, § 1, hiervan onverwijld in kennis.

§ 3. De bevoegde sectorale overheid stelt, nadat zij hiervan op de hoogte gebracht werd door de autoriteit bedoeld in artikel 21, § 1, de betrokken entiteit er onverwijld van in kennis dat zij als kritieke entiteit van bijzonder Europees belang wordt beschouwd.

Art. 15. Het Centraal Contactpunt, zoals bedoeld in artikel 21, § 1, is belast met het voeren van bilateraal en multilateraal overleg met de lidstaten van de Europese Unie inzake kritieke entiteiten:

a) die gebruik maken van een kritieke infrastructuur die fysiek verbonden is met twee of meer lidstaten;

b) die deel uitmaken van bedrijfsstructuren die verbonden zijn met of gekoppeld zijn aan kritieke entiteiten in andere lidstaten;

c) die in een lidstaat als zodanig zijn aangemerkt en essentiële diensten verlenen aan of in andere lidstaten.

Het overleg is erop gericht de weerbaarheid van kritieke entiteiten te vergroten en, waar mogelijk, de administratieve lasten voor de kritieke entiteiten te verminderen.

HOOFDSTUK 5 – Interne weerbaarheidsmaatregelen van de kritieke entiteit

Art. 16. § 1. De kritieke entiteit duidt een “contactpunt kritieke entiteit” aan en maakt de contactgegevens ervan over aan de sectorale overheid binnen een termijn van zes maanden vanaf de betekening van de aanduiding als kritieke entiteit, alsook na elke wijziging van deze gegevens.

§ 4. L’autorité visée à l’article 21, § 1, informe l’autorité nationale de cybersécurité visée à l’article 16 de la loi NIS 2 de la désignation des entités critiques.

Section 2. Entités critiques revêtant une importance européenne particulière

Art. 14. § 1er. Une entité est considérée comme une entité critique revêtant une importance européenne particulière pour autant qu’elle ait été désignée comme une entité critique conformément à l’article 12, qu’elle fournisse des services essentiels à ou dans plus de 6 États membres, et qu’elle ait été notifiée en vertu de l’article 13, § 1er de sa désignation en tant qu’entité critique.

§ 2. Suite à la notification de sa désignation conformément à l’article 13, § 1er, l’entité critique doit informer l’autorité sectorielle compétente lorsqu’elle fournit des services essentiels à ou dans plus de 6 États membres, quels sont les services essentiels qu’elle fournit à ou dans ces États membres, et à quels États membres elle fournit ces services essentiels.

L’autorité sectorielle en informe l’autorité visée à l’article 21, § 1er, sans délai.

§ 3. L’autorité sectorielle compétente, après avoir été informée par l’autorité visée à l’article 21, § 1er, notifie sans délai à l’entité concernée qu’elle est considérée comme une entité critique revêtant une importance européenne particulière.

Art. 15. Le Point de Contact Central, visé à l’article 21, § 1er, est chargé de mener des discussions bilatérales et multilatérales avec les États membres de l’Union européenne sur des entités critiques:

a) qui ont recours à une infrastructure critique qui est physiquement connectée avec deux États membres ou plus;

b) qui font partie de structures d’entreprise connectées ou liées à des entités critiques dans d’autres États membres;

c) qui sont identifiées comme telles dans un État membre et fournissent des services essentiels à ou dans d’autres États membres.

La concertation vise à accroître la résilience des entités critiques et, dans la mesure du possible, à réduire la charge administrative reposant sur les entités critiques.

CHAPITRE 5 – Mesures internes de la résilience de l’entité critique

Art. 16. § 1er. L’entité critique désigne un “point de contact de l’entité critique” et transfère ses coordonnées à l’autorité sectorielle dans un délai de six mois à compter de la notification de la désignation en tant qu’entité critique, ainsi qu’après chaque modification de ces données.

Het “contactpunt kritieke entiteit” oefent de functie uit van contactpunt ten aanzien van de sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, de burgermeester, de gouverneur, de politiediensten en elke andere bevoegde overheid of openbare dienst voor elke vraag in verband met de weerbaarheid van de entiteit en zijn infrastructuur.

§ 2. Indien er reeds een “contactpunt kritieke entiteit” werd aangeduid krachtens nationale of Europese bepalingen, maakt de kritieke entiteit de contactgegevens ervan over aan de sectorale overheid.

§ 3. Het “contactpunt kritieke entiteit” is te allen tijde beschikbaar.

Art. 17. § 1. De kritieke entiteit maakt een risicobeoordeling van alle relevante risico’s die de levering van haar essentiële diensten kunnen verstoren, binnen negen maanden na ontvangst van de in artikel 13, § 1, bedoelde kennisgeving, en vervolgens telkens wanneer dat nodig is, en ten minste om de vier jaar. Daarbij houdt ze rekening met de risicobeoordeling bedoeld in artikel 7, § 2, de dreigingsanalyse bedoeld in artikel 8 die het OCAD opstelt en andere relevante informatie.

§ 2. De risicobeoordeling van de kritieke entiteit zoals bedoeld in paragraaf 1, neemt de in artikel 7, § 3 bedoelde relevante risico’s in aanmerking die tot een incident zouden kunnen leiden. De risicobeoordeling houdt rekening met de mate waarin andere in Bijlage beschreven sectoren afhankelijk zijn van de door de kritieke entiteit verleende essentiële dienst, en de mate waarin die kritieke entiteit afhankelijk is van essentiële diensten van andere entiteiten in andere sectoren, in voorkomend geval tevens in naburige lidstaten en derde landen.

§ 3. Indien een kritieke entiteit reeds risicobeoordelingen heeft uitgevoerd of documenten heeft opgesteld krachtens andere wettelijke bepalingen die relevant zijn voor haar risicobeoordeling bedoeld in paragraaf 1, kunnen die beoordelingen en documenten gebruikt worden om aan de voorschriften van dit artikel te voldoen, voor zover deze betrekking hebben op de in artikel 7, § 3 bedoelde risico’s.

Art. 18. § 1. De kritieke entiteit werkt een weerbaarheidsplan van de entiteit uit, hierna W.P.E. genaamd, met het oog op het voorkomen, beperken en neutraliseren van de risico’s op verstoring van de werking of van de vernietiging van de kritieke entiteit en de weerbaarheid ervan te waarborgen, door het op punt stellen van interne passende en evenredige technische, veiligheids- en organisatorische maatregelen.

§ 2. Het W.P.E. bevat weerbaarheidsmaatregelen die toegepast worden in functie van de risico’s waaraan de entiteit kan worden blootgesteld, rekening houdend met de mogelijkheid tot wijzigende omstandigheden.

Voor een bepaalde sector, of in voorkomend geval, per deelsector, kan de Koning deze maatregelen specifiëren en opleggen om bepaalde informatie op te nemen in het W.P.E.

Le “point de contact de l’entité critique” remplit la fonction de point de contact vis-à-vis de l’autorité sectorielle, de l’autorité visée à l’article 21, § 1er, du bourgmestre, du gouverneur, des forces de police, et de tout autre autorité ou service public compétent, pour toute question liée à la résilience de l’entité et de son infrastructure.

§ 2. Si un “point de contact de l’entité critique” a été déjà désigné en vertu de dispositions nationales ou européennes, l’entité critique transfère ses coordonnées à l’autorité sectorielle.

§ 3. Le “point de contact de l’entité critique” est disponible à tout moment.

Art. 17. § 1er. L’entité critique procède à une évaluation de tous les risques pertinents susceptibles de perturber la fourniture de ses services essentiels, dans les neuf mois suivant la réception de la notification visée à l’article 13, § 1er, et par la suite chaque fois que nécessaire, et au moins tous les quatre ans. Ce faisant, elle tient compte de l’évaluation des risques visée à l’article 7, § 2 , de l’analyse de la menace effectuée par l’OCAM et visée à l’article 8 et d’autres informations pertinentes.

§ 2. L’évaluation des risques de l’entité critique, visée au paragraphe 1er, prend en considération les risques pertinents visés à l’article 7, § 3 qui pourraient conduire à un incident. L’évaluation des risques tient compte de la mesure dans laquelle d’autres secteurs décrits en Annexe dépendent du service fourni par l’entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d’autres entités dans d’autres secteurs, y compris, le cas échéant, dans les États membres voisins et les pays tiers.

§ 3. Si une entité critique a déjà effectué des évaluations de risques ou préparé des documents en vertu d’autres dispositions légales pertinentes pour son évaluation de risques visée au paragraphe 1er, ces évaluations et documents peuvent être utilisés pour se conformer aux exigences du présent article, dans la mesure où ils concernent les risques visés à l’article 7, § 3.

Art. 18. § 1er. L’entité critique élabore un plan de résilience de l’entité, ci-après dénommé P.R.E., en vue de prévenir, atténuer et neutraliser les risques d’interruption du fonctionnement ou de destruction de l’entité critique et d’assurer la résilience par la mise en place de mesures techniques, sécuritaires et organisationnelles internes appropriées et proportionnées.

§ 2. Le P.R.E. contient des mesures de résilience appliquées en fonction des risques auxquels l’entité peut être exposée, en tenant compte de la possibilité de changements de circonstances.

Pour un secteur donné, ou, le cas échéant, par sous-secteur, le Roi peut préciser ces mesures et imposer d’inclure certaines informations dans le P.R.E.

§ 3. Het W.P.E. bevat minstens:

1° een opsomming van weerbaarheidsmaatregelen, met inbegrip van maatregelen die nodig zijn om:

a) te voorkomen dat incidenten zich voordoen, rekening houdend met maatregelen ter beperking van het risico op rampen en maatregelen voor aanpassing aan de klimaatverandering;

b) te zorgen voor adequate fysieke bescherming van de gebouwen en kritieke infrastructuur, rekening houdend met het plaatsen van omheiningen, het oprichten van barrières, instrumenten en routines voor bewaking van de omgeving, detectieapparatuur en toegangscontroles;

c) de gevolgen van incidenten te bestrijden, te beperken en ertegen bestand te zijn, door te voorzien in aangepaste materiële en organisatorische noodmaatregelen en naar behoren rekening houdend met de uitvoering van de risico- en crisisbeheersingsprocedures en protocollen en waarschuwingsroutines, hetgeen de vorm kan aannemen van een intern noodplan;

d) te herstellen van incidenten, rekening houdend met bedrijfscontinuïteitsmaatregelen en de identificatie van alternatieve toeleveringsketens, teneinde de verlening van de essentiële dienst te hervatten;

e) te zorgen voor adequaat beheer van personeelsbeveiliging, rekening houdend met maatregelen zoals het vaststellen van categorieën personeelsleden die kritieke functies vervullen, het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en gevoelige informatie, het instellen van procedures voor veiligheidsverificaties zoals bedoeld in artikel 18 en het aanwijzen van categorieën van personen die aan een dergelijke veiligheidsverificatie moeten worden onderworpen, en het vaststellen van passende opleidingsvoorschriften en kwalificaties;

f) het relevante personeel bewust te maken van de hierboven vermelde maatregelen, naar behoren rekening houdend met opleidingen, informatiemateriaal en oefeningen;

2° de inventaris en de ligging van de kritieke infrastructuur, zoals bedoeld in artikel 9, § 2;

3° de risicobeoordeling vermeld in artikel 17;

§ 4. Binnen een termijn van uiterlijk tien maanden, te rekenen vanaf de betekening van de aanduiding van haar entiteit als kritieke entiteit zoals bedoeld in artikel 13, past de entiteit de weerbaarheidsmaatregelen uit het W.P.E. toe.

§ 5. Wanneer kritieke entiteiten uit hoofde van nationale of Europese wetgeving, documenten hebben opgesteld en maatregelen hebben genomen die van belang zijn voor de in paragraaf 3 bedoelde maatregelen, dan kunnen zij deze maatregelen en documenten gebruiken om te voldoen aan de voorschriften van dit artikel.

§ 3. Le P.R.E. contient au moins:

1° un énumération des mesures de résilience, y compris les mesures nécessaires pour:

a) prévenir les incidents, en tenant compte des mesures de réduction des risques de catastrophes et des mesures d'adaptation au changement climatique;

b) assurer une protection physique adéquate des bâtiments et des infrastructures critiques, en tenant compte de l'installation de clôtures, de barrières, d'outils et de routines de surveillance des environs, d'équipements de détection et de contrôles d'accès;

c) traiter, atténuer et résister aux conséquences des incidents, en prévoyant des mesures d'urgence matérielles et organisationnelles appropriées et en tenant dûment compte de la mise en œuvre des procédures et protocoles de gestion des risques et des crises et des routines d'alerte, ce qui peut prendre la forme d'un plan interne d'urgence;

d) pour se remettre d'un incident, en prenant en compte les mesures de continuité de l'activité et l'identification de chaînes d'approvisionnement alternatives afin de reprendre la fourniture du service essentiel;

e) assurer une gestion adéquate de la sécurité du personnel, en tenant compte de mesures telles que l'identification des catégories de personnel exerçant des fonctions critiques, l'établissement de droits d'accès aux bâtiments, aux infrastructures critiques et aux informations sensibles, l'établissement de procédures d'enquête de sécurité visée à l'article 18 et l'identification des catégories de personnes devant faire l'objet d'une telle enquête, ainsi que l'établissement d'exigences appropriées en matière de formation et de qualifications;

f) sensibiliser le personnel concerné aux mesures énumérées ci-dessus, en tenant dûment compte de la formation, du matériel d'information et des exercices;

2° l'inventaire et la localisation des infrastructures critiques visées à l'article 9, § 2;

3° l'évaluation des risques visée à l'article 17;

§ 4. Dans un délai maximum de dix mois à compter de la notification de la désignation de son entité comme entité critique visée à l'article 13, l'entité met en œuvre les mesures de résilience du P.R.E.

§ 5. Lorsque les entités critiques ont préparé des plans et des documents en vertu du droit national ou européen qui sont pertinents pour les mesures visées au paragraphe 3, elles peuvent utiliser ces documents pour se conformer aux exigences du présent article.

§ 6. De kritieke entiteit organiseert oefeningen en actualiseert het W.P.E. in functie van de lessen die getrokken worden uit deze oefeningen.

De Koning bepaalt, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de actualiseringen van het W.P.E.

De Koning bepaalt voor een bepaalde sector of, in voorkomend geval, per deelsector, de nadere regels van de deelneming van de relevante overheidsdiensten aan de oefeningen georganiseerd door de kritieke entiteit.

Art. 19. Op vraag van de bevoegde sectorale overheid of op eigen initiatief kunnen de kritieke entiteiten de procedure uit artikel 22*quinquies* van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst opstarten, teneinde de uitoefening van een beroep, functie, opdracht of mandaat, of toegang tot lokalen, gebouwen of terreinen afhankelijk te stellen van het ondergaan van een veiligheidsverificatie.

Art. 20. § 1. Onverminderd de wettelijke of reglementaire bepalingen die, in een bepaalde sector of deelsector, opleggen bepaalde diensten te informeren, is de kritieke entiteit ertoe gehouden, wanneer zich een gebeurtenis voordoet die van aard is om de verlening van essentiële diensten aanzienlijk te verstoren of kunnen verstoren, onmiddellijk het SICAD, via een rechtstreeks specifiek voorbehouden communicatiekanaal, de door de bevoegde sectorale overheid aangewezen dienst en de autoriteit bedoeld in artikel 21, § 1, te verwittigen.

Deze melding bevat alle beschikbare informatie die nodig is om te bepalen wat de aard, oorzaak en mogelijke gevolgen van het incident zijn, waaronder alle beschikbare informatie die nodig is om te bepalen of er grensoverschrijdende gevolgen zijn.

Om te bepalen of een verstoring aanzienlijk is, wordt rekening gehouden met:

1° het aantal getroffen gebruikers en hun aandeel;

2° de duur van de gebeurtenis;

3° het getroffen geografisch gebied.

In het geval van grensoverschrijdende gevolgen voor de verlening van essentiële diensten in andere lidstaten, meldt de kritieke entiteit dat aan de autoriteit bedoeld in artikel 21, § 1.

§ 2. Overeenkomstig de nadere regels bepaald door de minister van Binnenlandse Zaken, verwittigt het SICAD de autoriteit bedoeld in artikel 21, § 1, van elke gebeurtenis waarvan het kennis heeft en die van aard is de verlening van essentiële diensten van de kritieke entiteit aanzienlijk te verstoren en, in voorkomend geval, de autoriteit bedoeld in artikel 16 van de [NIS 2 wet].

§ 6. L'entité critique organise des exercices et met à jour le P.R.E., en fonction des enseignements tirés de ces exercices.

Le Roi détermine, pour un secteur ou sous-secteur donné, la fréquence des exercices et des mises à jour du P.R.E.

Le Roi détermine, pour un secteur donné ou, le cas échéant, par sous-secteur, les modalités de la participation des services publics concernés aux exercices organisés par l'entité critique.

Art. 19. À la demande de l'autorité sectorielle compétente ou de leur propre initiative, les entités critiques peuvent initier la procédure prévue à l'article 22*quinquies* de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé afin de soumettre l'exercice d'une profession, d'une fonction, d'une mission ou d'un mandat, ou l'accès à des locaux, des bâtiments ou des terrains à une vérification de sécurité.

Art. 20. § 1er. Sans préjudice des dispositions légales ou réglementaires qui imposent, dans un secteur ou sous-secteur donné, d'informer certains services, l'entité critique est tenue, lorsque survient un événement de nature à perturber ou risquant de perturber de manière importante la fourniture de services essentiels, d'en informer immédiatement le SICAD, par un canal de communication direct et spécifiquement réservé, le service désigné par l'autorité sectorielle compétente et l'autorité visée à l'article 21, § 1er.

Cette notification contient toutes les informations disponibles nécessaires pour déterminer la nature, la cause et les conséquences éventuelles de l'incident, y compris toutes les informations disponibles nécessaires pour déterminer s'il y a des implications transfrontalières.

Pour déterminer si une perturbation a un caractère important, il convient de prendre en compte des éléments suivants:

1° le nombre d'utilisateurs concernés et leur proportion;

2° la durée de l'événement;

3° la zone géographique concernée.

En cas d'effets transfrontaliers sur la fourniture de services essentiels dans d'autres États membres, l'entité critique en notifie l'autorité visée à l'article 21, § 1er.

§ 2. Conformément aux modalités fixées par le ministre de l'Intérieur, le SICAD notifie à l'autorité visée à l'article 21, § 1er, tout événement dont il a connaissance et qui est de nature à perturber de manière importante la fourniture des services essentiels de l'entité critique et, le cas échéant, l'autorité visée à l'article 16 de la [loi NIS 2].

§ 3. Indien de gebeurtenis van aard is om de verstoring van de werking of de vernietiging van de betrokken kritieke entiteit als gevolg te hebben, verwittigt het Centraal Contactpunt de bevoegde sectorale overheid en, in het geval het incident aanzienlijke gevolgen heeft of kan hebben voor kritieke entiteiten en voor de continuïteit van de verlening van essentiële diensten in één of meer lidstaten, de bevoegde overheid van de betrokken lidstaten.

HOOFDSTUK 6 – Rapportage en informatie-uitwisseling

Afdeling 1. De bevoegde autoriteiten

Art. 21. § 1. De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit bedoeld in het eerste lid is ook het Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de lidstaten van de Europese Unie.

Daartoe vertegenwoordigt het contactpunt België binnen de Groep voor de weerbaarheid van kritieke entiteiten.

§ 2. De autoriteit bedoeld in de eerste paragraaf coördineert en voldoet aan de rapportageverplichtingen die voortvloeien uit hoofde van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad inzake de weerbaarheid van kritieke entiteiten.

§ 3. De Koning kan de coördinerende rol van de autoriteit als bedoeld in de eerste paragraaf voor wat betreft de weerbaarheid van kritieke entiteiten verder preciseren.

§ 4. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de nadere regels bepaald in artikel 92*ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden aan.

Art. 22. De Koning wijst de autoriteit aan die belast is met het opstellen van een nationale strategie om de weerbaarheid van kritieke entiteiten te verbeteren. Deze strategie wordt uiterlijk op 17 januari 2026, en daarna ten minste om de vier jaar opgesteld.

De autoriteit bedoeld in het eerste lid raadpleegt, in voorkomend geval, de sectorale overheden, de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-wet en de gefedereerde entiteiten.

§ 3. Si l'événement est de nature à entraîner l'interruption du fonctionnement ou la destruction de l'entité critique concernée, le Point de Contact Central en informe l'autorité sectorielle compétente et, dans le cas où l'incident a ou peut avoir un impact important sur les entités critiques et sur la continuité de la fourniture des services essentiels dans un ou plusieurs États membres, l'autorité compétente des États membres concernés.

CHAPITRE 6 – Rapports et échange d'informations

Section 1re. Les autorités compétentes

Art. 21. § 1er. Le Roi désigne l'autorité qui, en tant qu'autorité nationale, est chargée du suivi et de la coordination de la mise en œuvre de la présente loi.

L'autorité visée au premier alinéa est également le Point de Contact Central National pour la résilience des entités critiques, pour l'ensemble des secteurs et sous-secteurs, pour la Belgique dans sa relation avec la Commission européenne et les États membres de l'Union européenne.

À cette fin, le point de contact représente la Belgique au sein du Groupe pour la résilience des entités critiques.

§ 2. L'autorité visée au premier paragraphe coordonne et respecte les obligations d'information découlant de la directive (UE) 2022/2557 du Parlement européen et du Conseil relative à la résilience des entités critiques.

§ 3. Le Roi peut préciser le rôle de coordination de l'autorité visée au paragraphe 1er en ce qui concerne la résilience des entités critiques.

§ 4. Le Roi désigne, par arrêté pris après avis du Conseil des ministres, les autorités sectorielles chargées, pour leur secteur respectif, de veiller à l'exécution des dispositions de la présente loi.

Le Roi peut instituer des autorités sectorielles composées de représentants de l'État fédéral, des Communautés et des Régions, selon les modalités prévues à l'article 92*ter* de la loi spéciale du 8 août 1980 sur la réforme institutionnelle.

Nonobstant le premier alinéa, cette loi désigne elle-même les autorités sectorielles établies et réglementées par la loi.

Art. 22. Le Roi désigne l'autorité chargée d'établir une stratégie nationale visant à améliorer la résilience des entités critiques. Cette stratégie est établie au plus tard le 17 janvier 2026, et au moins tous les quatre ans par la suite.

L'autorité visée à l'alinéa 1er consulte, le cas échéant, les autorités sectorielles, l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 et les entités fédérées.

De nationale strategie bevat minstens:

1° strategische doelstellingen en prioriteiten ter vergroting van de algehele weerbaarheid van kritieke entiteiten, met inachtneming van grensoverschrijdende, intersectorale en onderlinge afhankelijkheden;

2° een *governance* kader ter verwezenlijking van de strategische doelstellingen en prioriteiten, met inbegrip van een beschrijving van de taken en verantwoordelijkheden van de verschillende autoriteiten, kritieke entiteiten en andere partijen die bij de uitvoering van de strategie betrokken zijn;

3° een beschrijving van de maatregelen die nodig zijn om de algehele weerbaarheid van kritieke entiteiten te vergroten, inclusief een beschrijving van de nationale risicobeoordeling;

4° een beschrijving van het proces waarmee kritieke entiteiten worden geïdentificeerd;

5° een beschrijving van het proces waarmee kritieke entiteiten worden ondersteund, met inbegrip van maatregelen ter verdieping van de samenwerking tussen de publieke sector enerzijds en de particuliere sector en de publieke en particuliere entiteiten anderzijds;

6° een lijst van de belangrijkste autoriteiten en belanghebbenden, met uitzondering van de kritieke entiteiten, die betrokken zijn bij de uitvoering van de strategie;

7° een beleidskader voor de coördinatie tussen de in deze wet bevoegde autoriteiten en de overeenkomstig de NIS 2 wet aangewezen bevoegde autoriteiten, met het oog op de uitwisseling van informatie over cyberbeveiligingsrisico's, cyberdreigingen en -incidenten en niet-cyber gerelateerde risico's, dreigingen en incidenten en de uitoefening van toezichthoudende taken;

8° een beschrijving van de reeds bestaande maatregelen om de uitvoering van de verplichtingen uit hoofde van Hoofdstuk 5 door kleine en middelgrote ondernemingen in de zin van de bijlage bij de Commissieaanbeveling 2003/361/EC25, die de lidstaten als kritieke entiteiten hebben aangemerkt, te vergemakkelijken

Afdeling 2. Informatie-uitwisseling

Art. 23. De autoriteit bedoeld in artikel 21, § 1, het OCAD en, in voorkomend geval, de autoriteit bedoeld in artikel 16 [NIS 2 Wet] en de sectorale overheid wisselen vanuit hun eigen bevoegdheden, alle nuttige informatie uit voor het nemen van externe beschermingsmaatregelen voor de kritieke entiteiten.

Art. 24. § 1. De kritieke entiteit, het contactpunt kritieke entiteit, de sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, het OCAD, en, in voorkomend geval, de autoriteit bedoeld in artikel 16 [NIS 2 wet], werken te allen tijde samen, vanuit hun eigen opdracht en bevoegdheden, door middel van een adequate informatie-uitwisseling betreffende de weerbaarheid

La stratégie nationale comprend au moins:

1° des objectifs et priorités stratégiques visant à renforcer la résilience globale des entités critiques en tenant compte des aspects transfrontaliers, intersectoriels et des interdépendances;

2° un cadre de gouvernance pour atteindre les objectifs et priorités stratégiques, y compris une description des rôles et responsabilités des différentes autorités, entités critiques et autres parties impliquées dans la mise en œuvre de la stratégie;

3° une description des mesures nécessaires pour accroître la résilience globale des entités critiques, y compris une description de l'évaluation nationale des risques;

4° une description du processus d'identification des entités critiques;

5° une description du processus de soutien, y compris les mesures visant à approfondir la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part;

6° une liste des principales autorités et parties concernées, à l'exclusion des entités critiques, qui participent à la mise en œuvre de la stratégie;

7° un cadre politique pour la coordination entre les autorités compétentes en vertu de la présente loi et les autorités compétentes désignées conformément à la loi NIS 2, aux fins de l'échange d'informations sur les risques, les menaces et les incidents liés à la cybersécurité et les risques, menaces et incidents non liés à la cybersécurité et l'exercice des fonctions de surveillance;

8° une description des mesures déjà en place pour faciliter la mise en œuvre des obligations du Chapitre 5 par les petites et moyennes entreprises au sens de l'annexe de la Recommandation 2003/361/CE25 de la Commission, que les États membres ont identifiées comme des entités critiques**.**

Section 2. Échange d'informations

Art. 23. L'autorité visée à l'article 21, § 1er, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi du [NIS 2] et l'autorité sectorielle s'échangent, dans le cadre de leurs compétences, toute information utile pour la prise de mesures externes de protection des entités critiques.

Art. 24. § 1er. L'entité critique, le point de contact de l'entité critique, l'autorité sectorielle, l'autorité visée à l'article 21, § 1er, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi du [NIS 2] collaborent en tout temps, dans le cadre de leurs mandat et compétences, par un échange adéquat d'informations concernant la résilience de l'entité critique, afin

van de kritieke entiteiten, teneinde te waken over een overeenstemming tussen de interne weerbaarheidsmaatregelen en de externe beschermingsmaatregelen.

§ 2. De sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, en de kritieke entiteit kunnen, in voorkomend geval, informatie uitwisselen met de gefedereerde entiteiten, voor de kritieke entiteiten die onder hun bevoegdheden vallen.

Art. 25. De Koning kan, voor een bepaalde sector, of in voorkomend geval, per deelsector, de informatie bepalen die pertinent kan zijn voor het vervullen van de opdrachten van de autoriteit bedoeld in artikel 21, § 1, en van het OCAD op het vlak van de weerbaarheid van kritieke entiteiten, en de nadere regels van de toegang tot die informatie bepalen.

Art. 26. De autoriteit bedoeld in artikel 21, § 1, kan aan de kritieke entiteit informatie over de dreiging en over de externe beschermingsmaatregelen overmaken die de entiteit toelaten zijn weerbaarheidsmaatregelen op gepaste wijze toe te passen en ze in overeenstemming te brengen met de externe beschermingsmaatregelen.

De autoriteit bedoeld in artikel 21, § 1, kan een kopie van deze informatie aan de bevoegde sectorale overheid overzenden.

Art. 27. De sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, het OCAD, en de autoriteit bedoeld in artikel 16 [NIS 2 wet] beperken de toegang tot de informatie bedoeld in Hoofdstukken 4 en 5, tot de personen die er kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht in het kader van de weerbaarheid van de kritieke entiteiten, zoals bedoeld in deze wet.

Art. 28. § 1. Onverminderd artikel 25 is de kritieke entiteit gehouden tot het beroepsgeheim voor wat de inhoud van het W.P.E. betreft en mag zij enkel toegang geven tot het W.P.E. aan personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht.

De kritieke entiteit is aan hetzelfde geheim gehouden voor wat betreft alle informatie die haar ter kennis wordt gebracht met toepassing van Hoofdstuk 4, artikel 18, § 6, en de artikelen 20, 24, en 26.

§ 2. Inbreuken op paragraaf 1 worden bestraft met de straffen voorzien bij artikel 458 van het Strafwetboek.

Art. 29. De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op informatie, documenten of gegevens, in welke vorm ook, bedoeld in artikel 27.

Art. 30. § 1. De sectorale overheid waakt erover dat minstens één iemand van zijn personeel dat toegang heeft tot informatie inzake de weerbaarheid van kritieke entiteiten, zoals bedoeld in de Hoofdstukken 4 en 5 van deze wet, beschikt over een veiligheidsmachtiging van het niveau GEHEIM, als bedoeld in Hoofdstuk III van de wet van 11 december 1998 betreffende de

de veiller à une concordance entre les mesures internes de résilience et les mesures externes de protection.

§ 2. L'autorité sectorielle, l'autorité visée à l'article 21, § 1er, et l'entité critique peuvent, le cas échéant, échanger des informations avec les entités fédérées, pour les entités critiques relevant de leur compétence.

Art. 25. Le Roi peut déterminer, pour un secteur déterminé ou, le cas échéant, par sous-secteur, les informations qui peuvent être pertinentes pour l'accomplissement des missions de l'autorité visée à l'article 21, § 1er, et de l'OCAM en matière de protection des entités critiques, ainsi que les modalités d'accès à ces informations.

Art. 26. L'autorité visée à l'article 21, § 1er, peut communiquer à l'entité critique des informations relatives à la menace et aux mesures externes de protection qui permettent à l'entité d'appliquer ses mesures de résilience de manière appropriée et de les mettre en concordance avec les mesures externes de protection.

L'autorité visée à l'article 21, § 1er, peut transmettre une copie de ces informations à l'autorité sectorielle compétente.

Art. 27. L'autorité sectorielle, l'autorité visée à l'article 21, § 1er, l'OCAM, et l'autorité visée à l'article 16 de la loi [NIS 2] limitent l'accès aux informations visées aux Chapitres 4 et 5, aux personnes ayant besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission, dans le contexte de la résilience des entités critiques, telle que visée dans la présente loi.

Art. 28. § 1er. Sans préjudice de l'article 25, l'entité critique est tenue au secret professionnel en ce qui concerne le contenu du P.R.E. et ne peut donner accès au P.R.E. qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission.

L'entité critique est tenue au même secret en ce qui concerne toutes les informations portées à sa connaissance en application du Chapitre 4, article 18, § 6, et des articles 20, 24, et 26.

§ 2. Les infractions au paragraphe 1er sont punies des peines prévues à l'article 458 du Code pénal.

Art. 29. La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés à l'article 27.

Art. 30. § 1er. L'autorité sectorielle veille à ce qu'au moins une personne de son personnel ayant accès aux informations relatives à la résilience des entités critiques, visées aux Chapitres 4 et 5 de la présente loi, dispose d'une habilitation de sécurité de niveau SECRET, telle que visée au Chapitre III de la loi du 11 décembre 1998 relative à la classification, aux

classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst. De Koning kan, voor een bepaalde sector of deelsector, nadere regels hieromtrent vastleggen.

§ 2 De Koning kan, op voordracht van de bevoegde minister, de classificatie van een deel of van het geheel van het W.P.E. voorzien. Hij houdt er rekening mee dat de bevoegde personen binnen de kritieke entiteit ten allen tijde toegang hebben tot hun volledige W.P.E.

HOOFDSTUK 7 – Controle en sancties

Afdeling 1. Inspecties en audits

Art. 31. § 1. De Koning stelt per sector, of, in voorkomend geval, per deelsector, een inspectiedienst aan, belast met de controle op de naleving, door de kritieke entiteiten van die sector of deelsector, van de bepalingen van deze wet en van haar uitvoeringsbesluiten.

§ 2. De Koning legt de nadere regels van deze controle vast. Deze nadere regels bevatten onder andere de opdrachten van de inspectiedienst, de frequentie van de controles, de minimale voorwaarden waaraan de inspecteleden moeten voldoen en de punten waarop de controle dient te gebeuren, of de rapportering die aan de sectorale overheid moeten worden gedaan.

Art. 32. De Koning legt, voor een bepaalde sector, of in voorkomend geval, per deelsector, nadere regels vast met betrekking tot het opleggen en de uitvoering van audits ten aanzien van kritieke entiteiten

Afdeling 2. Procedure van de sancties

Art. 33. § 1. Wanneer een of meer inbreuken op de eisen van de wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kan de inspectiedienst de betrokken kritieke entiteit in gebreke stellen om zijn verplichtingen na te komen binnen een door hem vastgestelde termijn.

De termijn wordt bepaald, rekening houdend met de werkings-voorwaarden van de kritieke entiteit en met de te nemen maatregelen.

§ 2. De inspectiedienst kan de overtreder vooraf, op een met redenen omklede wijze, meedelen dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de inspectiedienst.

Art. 34. § 1. Als de inspectiedienst vaststelt dat de kritieke entiteit geen gevolg geeft aan de ingebrekestelling binnen de vastgestelde termijn, worden de feiten vastgesteld in een

habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé. Le Roi peut, pour un secteur ou sous-secteur déterminé, fixer d'autres règles à cet égard.

§ 2 Le Roi peut, sur proposition du ministre compétent, prévoir la classification de tout ou partie du P.R.E. Ce faisant, il tient compte du fait que les personnes compétentes au sein de l'entité critique ont à tout moment accès à l'ensemble de leur P.R.E.

CHAPITRE 7 – Contrôle et sanctions

Section 1re. Inspections et audits

Art. 31. § 1er. Le Roi institue un service d'inspection par secteur, ou, le cas échéant, par sous-secteur, chargé du contrôle du respect des dispositions de la présente loi et de ses arrêtés d'exécution par les entités critiques dudit secteur ou sous-secteur.

§ 2. Le Roi fixe les modalités de ce contrôle. Ces modalités comprennent notamment les missions du service d'inspection, la fréquence des inspections, les conditions minimales à remplir par les membres de l'inspection et les points à inspecter, ou le rapportage à faire aux autorités sectorielles.

Art. 32. Le Roi fixe, pour un secteur particulier ou, le cas échéant, par sous-secteur, des règles supplémentaires concernant l'imposition et la réalisation d'audits à l'égard d'entités critiques.

Section 2. Procédure de sanctions

Art. 33. § 1er. Lorsqu'une ou plusieurs infractions aux exigences de la loi, de ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes sont constatées, le service d'inspection peut mettre en demeure l'entité critique concernée de remplir ses obligations dans un délai qu'elle fixe.

Le délai est déterminé en tenant compte des conditions d'exploitation de l'entité critique et des mesures à prendre.

§ 2. Le service d'inspection peut notifier préalablement au contrevenant, de manière motivée, son intention de lui adresser une mise en demeure et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de cette information, de présenter ses moyens de défense par écrit ou de demander à être entendu. L'information est réputée avoir été reçue par le contrevenant le sixième jour après son envoi par le service d'inspection.

Art. 34. § 1er. Si le service d'inspection constate que l'entité critique ne se conforme pas à la mise en demeure dans le délai imparti, les faits sont constatés dans un rapport officiel

door de inspectiedienst opgesteld proces-verbaal. Een kopie van het proces-verbaal wordt naar de bevoegde sectorale overheid gestuurd.

§ 2. De inspectiedienst stuurt het origineel van het proces-verbaal naar de Procureur des Konings.

Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.

§ 3. De processen-verbaal hebben bewijskracht tot het tegendeel bewezen is.

Art. 35. Inbreuken op deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke of administratieve sancties.

Art. 36. De Procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging is ingesteld.

De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten voor het verstrijken van voorgemelde termijn, behalve wanneer de Procureur des Konings vooraf meedeelt dat hij geen gevolg aan de inbreuk wenst te geven.

Wanneer de Procureur des Konings geen kennis geeft van zijn beslissing binnen de vastgestelde termijn of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.

Art. 37. In afwijking van deze afdeling kan voor de sector vervoer over water, voor inbreuken op deze wet en haar uitvoeringsbesluiten, een administratieve geldboete worden opgelegd met toepassing boek 4 van het Belgisch scheepvaartwetboek en de wet van 25 december 2016 tot instelling van administratieve geldboetes van toepassing in geval van inbreuken op de scheepvaartwetten. De minimale en maximale bedragen van de administratieve geldboete stemmen overeen met de respectieve minimale en maximale bedragen voorzien in afdeling 4.

Afdeling 3. Strafrechtelijke sancties

Art. 38. § 1. Wordt gestraft met een gevangenisstraf van acht dagen tot een jaar en met een geldboete van 26 euro tot 10.000 euro of met één van die straffen alleen, de kritieke entiteit die de verplichtingen opgelegd door of krachtens deze wet betreffende de interne weerbaarheidsmaatregelen uit Hoofdstuk 3 en de uitwisseling van informatie uit Hoofdstuk 4, Afdeling 2, niet naleeft.

In geval van herhaling wordt de geldboete verdubbeld en wordt de overtreder gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.

§ 2. Wordt gestraft met gevangenisstraf van acht dagen tot een maand en met geldboete van 26 euro tot 1.000 euro of met één van die straffen alleen, eenieder die de uitvoering

rédigé par le service d'inspection. Une copie du rapport officiel est envoyée à l'autorité sectorielle compétente.

§ 2. Le service d'inspection envoie l'original du procès-verbal au Procureur du Roi.

En même temps, une copie du procès-verbal est envoyée à l'auteur de l'infraction.

§ 3. Les procès-verbaux ont valeur probante jusqu'à preuve du contraire.

Art. 35. Les violations de cette loi ou de ses décrets d'application peuvent donner lieu à des sanctions pénales ou administratives.

Art. 36. Le Procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour informer l'autorité sectorielle que des poursuites pénales ont été engagées.

L'autorité sectorielle ne peut entamer la procédure d'imposition d'une amende administrative avant l'expiration du délai susmentionné, à moins que le Procureur ne notifie au préalable qu'il ne souhaite pas donner suite à l'infraction.

Si le Procureur du Roi ne notifie pas sa décision dans le délai imparti ou s'il renonce aux poursuites pénales, l'autorité sectorielle peut décider d'engager la procédure administrative.

Art. 37. Par dérogation à la présente section, pour le secteur du transport par voie d'eau, en cas d'infraction à la présente loi et à ses arrêtés d'exécution, une amende administrative peut être imposée en application du livre 4 du Code de la marine marchande et de la loi du 25 décembre 2016 fixant les amendes administratives applicables en cas d'infraction à la législation sur la marine marchande. Les montants minimum et maximum de l'amende administrative correspondent aux montants minimum et maximum respectifs prévus à la section 4.

Section 3. Sanctions pénales

Art. 38. § 1er. Est punie d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 10.000 euros, ou de l'une de ces peines seulement, l'entité critique qui ne respecte pas les obligations imposées par ou en vertu de la présente loi, relatives aux mesures internes de résilience prévues au Chapitre 2 et à l'échange d'informations prévu au Chapitre 4, Section 2.

En cas de récidive, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans.

§ 2. Est puni d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 euros à 1.000 euros, ou de l'une de ces peines seulement, quiconque empêche ou

van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt.

In geval van herhaling, wordt de geldboete verdubbeld en de overtreder gestraft met een gevangenisstraf van vijftien dagen tot een jaar.

§ 3. De bepalingen van boek I van het Strafwetboek, met inbegrip van Hoofdstuk VII en artikel 85, zijn van toepassing op de vermelde inbreuken.

Afdeling 4. Administratieve sancties

Art. 39. § 1. Elke inbreuk op deze wet, op de uitvoeringsbesluiten of op de administratieve beslissingen die krachtens deze wet genomen worden, kan aanleiding geven tot een administratieve sanctie.

§ 2. Niet-naleving van de verplichtingen betreffende informatie-uitwisseling opgelegd krachtens artikel 9, § 3, wordt bestraft met een geldboete van 500 tot 75.000 euro.

§ 3. Niet-naleving van de verplichtingen betreffende de weerbaarheidsmaatregelen opgelegd door of krachtens Hoofdstuk 5 van deze wet, wordt bestraft met een geldboete van 500 tot 100.000 euro.

§ 4. Niet-naleving van de verplichtingen betreffende de uitwisseling van informatie uit Hoofdstuk 6, Afdeling 2, worden bestraft met een geldboete van 500 tot 100.000 euro.

§ 5. Niet-naleving van de verplichtingen betreffende de uitvoering van inspecties en audits opgelegd krachtens Hoofdstuk 7 van deze wet, wordt bestraft met een geldboete van 500 tot 125.000 euro.

Eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, die informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt bestraft met een geldboete van 500 tot 125.000 euro.

Art. 40. § 1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de sectorale overheid.

entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou communique sciemment des informations inexactes ou incomplètes.

En cas de récidive, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à un an.

§ 3. Les dispositions du livre 1er du Code pénal, en ce compris le Chapitre VII et l'article 85, sont applicables aux dites infractions.

Section 4. Sanctions administratives

Art. 39. § 1er. Toute violation de la présente loi, des décrets d'application ou des décisions administratives prises en vertu de la présente loi peut donner lieu à une sanction administrative.

§ 2. Le non-respect des obligations en matière d'échange d'informations imposées en vertu de l'article 9, § 3, est puni d'une amende allant de 500 à 75.000 euros.

§ 3. Le non-respect des obligations relatives aux mesures de résilience imposées par ou en vertu du Chapitre 5 de la présente loi est puni d'une amende de 500 à 100.000 euros.

§ 4. Le non-respect des obligations relatives à l'échange d'informations prévues au Chapitre 6, Section 2, est puni d'une amende de 500 à 100.000 euros.

§ 5. Le non-respect des obligations relatives à la conduite des inspections et des audits imposées en vertu du Chapitre 7 de la présente loi est puni d'une amende de 500 à 125.000 euros.

Quiconque empêche ou gêne volontairement la réalisation de l'inspection effectuée par les membres du service d'inspection, qui refuse de communiquer les informations qui lui sont demandées à la suite de cette inspection, ou qui communique délibérément des informations erronées ou incomplètes, est puni d'une amende de 500 à 125.000 euros.

Art. 40. § 1er. La décision d'infliger une amende administrative est motivée. Elle indique également le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité sectorielle communique au préalable au contrevenant sa proposition motivée de sanction administrative et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de la proposition, de présenter ses moyens de défense par écrit ou de demander à être entendu. La proposition est réputée avoir été reçue par le contrevenant le sixième jour suivant son envoi par l'autorité sectorielle.

§ 3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen dezelfde termijn, kan de sectorale overheid een in artikel 39 bedoelde administratieve sanctie opleggen.

§ 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.

De administratieve geldboete wordt verdubbeld in geval van herhaling binnen een termijn van drie jaar.

§ 5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 41. De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.

Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.

Art. 42. § 1. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de sectorale overheid of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het dient gedaan te worden door middel van een dagvaarding aan de sectorale overheid bij deurwaarderexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van Hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging van het dwangbevel, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§ 3. En tenant compte des moyens de défense soulevés dans le délai visé au paragraphe 2 ou en l'absence de réponse du contrevenant dans le même délai, l'autorité sectorielle peut imposer une sanction administrative visée à l'article 39.

§ 4. L'amende administrative est proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de l'infraction.

L'amende administrative est doublée en cas de récidive dans un délai de trois ans.

§ 5. La concomitance de plusieurs infractions peut donner lieu à une seule amende administrative proportionnelle à la gravité de l'infraction dans son ensemble.

Art. 41. La décision est notifiée au contrevenant par lettre recommandée.

Une demande de paiement de l'amende dans un délai d'un mois est jointe à la décision.

Art. 42. § 1er. Si le contrevenant ne paie pas l'amende administrative dans le délai imparti, la décision d'imposer une amende administrative est exécutoire et l'autorité sectorielle peut émettre une injonction.

L'injonction est délivrée par le représentant légal de l'autorité sectorielle ou par un agent habilité.

§ 2. L'injonction est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un ordre de payer dans les vingt-quatre heures sous peine d'exécution par saisie, ainsi qu'un relevé des sommes réclamées et une copie de la déclaration constatant la force exécutoire.

§ 3. L'auteur de l'infraction peut faire opposition à l'injonction auprès du juge des saisies.

Sous peine de nullité, l'opposition est motivée. Elle doit être faite par voie d'assignation à l'autorité sectorielle par exploit d'huissier dans les quinze jours à compter de la signification de l'injonction.

Les dispositions du Chapitre VIII de la première partie du Code judiciaire s'appliquent à ce délai, y compris les prolongations prévues à l'article 50, deuxième alinéa, et à l'article 55 de ce Code.

Le recours à l'opposition à l'injonction suspend l'exécution de l'injonction, ainsi que la prescription des créances visées par l'injonction, jusqu'à ce qu'il soit statué sur son bien-fondé. Les saisies déjà effectuées maintiennent leur caractère conservatoire.

§ 4. De sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Deze kosten worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 43. De sectorale overheid kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

De betaling volgens de administratieve procedures doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.

HOOFDSTUK 8 – Sector overheid

Art. 44. De Koning bepaalt voor de sector overheid, op voordracht van de sectoraal bevoegde minister, de wijze van uitvoering van de verplichtingen uit tenminste onderstaande bepalingen uit deze wet:

— artikel 7;

— artikel 9, § 1 en § 4;

— artikel 10;

— artikel 12, § 3;

— artikel 13;

— artikel 14;

— artikel 16;

— artikel 17;

— artikel 18, §§ 1 t.e.m. 5;

— artikel 19;

— artikel 20;

— artikel 31;

— artikel 32.

§ 4. L'autorité sectorielle peut ordonner des saisies conservatoires et exécuter l'injonction en utilisant les moyens d'exécution prévus dans la Cinquième partie du Code Judiciaire.

Les paiements partiels effectués à la suite de la signification d'une injonction ne font pas obstacle à la poursuite de l'action publique.

§ 5. Les frais de signification de l'injonction ainsi que les frais d'exécution ou de mesures conservatoires sont à la charge du contrevenant.

Ces frais sont déterminés selon les règles applicables aux actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 43. L'autorité sectorielle ne peut imposer une amende administrative après l'expiration d'une période de trois ans à compter du jour où l'infraction a été commise.

Le paiement dans le cadre de procédures administratives rend également caduque la possibilité de poursuites pénales pour les infractions en question.

CHAPITRE 8 – Secteur des administrations publiques

Art. 44. Le Roi détermine pour le secteur des administrations publiques, sur proposition du ministre sectoriel compétent, les modalités d'exécution des obligations découlant au moins des dispositions suivantes de la présente loi:

— article 7;

— article 9, § 1er et § 4;

— article 10;

— article 12, § 3;

— article 13;

— article 14;

— article 16;

— article 17;

— article 18, §§ 1 à 5;

— article 19;

— article 20;

— article 31;

— article 32.

HOOFDSTUK 9 – Diverse bepalingen

Afdeling 1. Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 45. In artikel 28/3, § 2, eerste lid, de bepaling onder 4° van de wet van 13 juni 2005 betreffende de elektronische communicatie, ingevoegd bij wet van 21 december 2021, worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

Art. 46. In artikel 105, § 2, de bepaling onder 2° van dezelfde wet, ingevoegd bij wet van 17 februari 2022, worden de woorden "exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "kritieke entiteit in de zin van de wet [*datum*] betreffende de weerbaarheid van kritieke entiteiten".

Art. 47. In artikel 126/3, § 3, de bepaling onder j), van dezelfde wet, ingevoegd bij wet van 20 juli 2022, worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 2. Wijzigingen van de wet van 14 februari 2023 houdende de instemming met het samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen

Art. 48. In artikel 4, van de wet van 14 februari 2023 houdende de instemming met het samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaamse Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, 2°, de bepaling onder a) worden de woorden "kritieke infrastructuur" vervangen door de woorden "kritieke entiteiten";

2° in paragraaf 2, 2°, de bepaling onder a) wordt het zinsdeel "in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, en in het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" vervangen als volgt: "in de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

CHAPITRE 9 – Dispositions diverses

Section 1re. Modification de la loi du 13 juin 2005 relative aux communications électroniques

Art. 45. À l'article 28/3, § 2, premier alinéa, la disposition sous 4° de la loi du 13 juin 2005 relative aux communications électroniques, inséré par la loi du 21 décembre 2021, les mots "la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "la loi du [date] relative à la résilience des entités critiques";

Art. 46. À l'article 105, § 2, la disposition sous 2° de la même loi, inséré par la loi du 17 février 2022, les mots "exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "entité critique au sens de la loi [*date*] relative à la résilience des entités critiques".

Art. 47. À l'article 126/3, paragraphe 3, la disposition sous j), de la même loi, insérée par la loi du 20 juillet 2022, les mots "la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et leurs décrets d'application" sont remplacés par les mots "la loi du [date] relative à la résilience des entités critiques.

Section 2. Modification de la loi du 14 février 2023 portant approbation de l'accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire mixte instituant un mécanisme de filtrage des investissements directs étrangers

Art. 48. À l'article 4 de la loi du 14 février 2023 portant approbation de l'accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire mixte instituant un mécanisme de filtrage des investissements directs étrangers, sont apportées les modifications suivantes:

1° au paragraphe 2, 2°, la disposition prévue au point a), les mots "infrastructures critiques" sont remplacés par les mots "entités critiques";

2° au paragraphe 2, 2°, la disposition prévue au point a), le membre de phrase "dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, et dans l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien" est remplacé comme suit: "dans la loi du [date] relative à la résilience des entités critiques".

Art. 49. In artikel 7 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° In paragraaf 4 worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”;

2° in paragraaf 4 worden de woorden “kritieke infrastructuur” vervangen door de woorden “kritieke entiteiten”.

Afdeling 3. Wijziging van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

Art. 50. In artikel 3, § 3, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit worden de woorden “in artikel 6, 2°, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, in artikel 3, 3°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 2, eerste lid, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer” vervangen door de woorden “in artikel 3, 2°, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”.

Art. 51. In artikel 6 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de paragrafen 2 en 3 worden de woorden “de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “de artikelen 3, 2°, en 31, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”;

2° in dezelfde paragrafen worden de woorden “in artikel 7, §§ 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” telkens vervangen door de woorden “in artikel 15, § 2, van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”;

3° in paragraaf 3 worden de woorden “en 15, §§ 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer” opgeheven.

4° in dezelfde paragraaf worden de woorden “de artikelen 20, 21, § 1, en 33, van de voormelde wet van 7 april 2019” vervangen door de woorden “de artikel 30 van de voormelde wet van […]”.

Art. 49. Les modifications suivantes sont apportées à l’article 7 de la même loi:

1° au paragraphe 4, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du [date] relative à la résilience des entités critiques”;

2° au paragraphe 4, les mots “infrastructures critiques” sont remplacés par les mots “entités critiques”.

Section 3. Modification de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l’information et la communication et désignant une autorité nationale de certification de cybersécurité

Art. 50. Dans l’article 3, § 3, de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l’information et de la communication et désignant une autorité nationale de certification de cybersécurité, les mots “l’article 6, 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, de l’article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et de l’article 2, alinéa 1er, 1°, de l’arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien” sont remplacés par les mots “à l’article 3, 2°, de la loi du [date] relative à la résilience des entités critiques”.

Art. 51. À l’article 6 de la même loi, les modifications suivantes sont apportées:

1° aux paragraphes 2 et 3, les mots “articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “articles 3, 2° et 31 de la loi du [date] relative à la résilience des entités critiques”;

2° dans les même paragraphes, les mots “à l’article 7, §§ 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont chaque fois remplacés par les mots “ou à l’article 15, § 2, de la loi du […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique”;

3° au paragraphe 3, les mots “et 15, §§ 1 à 3, de l’arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien” sont supprimés.

4° dans le même paragraphe, les mots “aux articles 20, 21, § 1er, et 33, de la loi précitée du 7 avril 2019” sont remplacés par les mots “à l’article 30 de la loi précitée du […]”.

Art. 52. In artikel 16, § 4, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden “artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “artikel 18 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”;

2° in het eerste lid worden de woorden “de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011” vervangen door de woorden “de artikelen 3, 2° en 31, van de voormelde wet van [datum]”;

3° in het eerste lid worden de woorden “de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en”, “en in artikel 7, §§ 3 en 5, van de voormelde wet van 7 april 2019”, “, een aanbieder van essentiële diensten of een digitaledienstverlener” en “of de voormelde wet van 7 april 2019” opgeheven;

4° in het tweede lid worden de woorden “kritieke infrastructuur” vervangen door de woorden “kritieke entiteiten”;

5° in het tweede lid wordt de bepaling onder 2° vervangen als volgt: “de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”;

Art. 53. In artikel 17, § 3, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden “en de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” opgeheven;

2° in hetzelfde lid worden de woorden “n in artikel 7, §§ 3 en 5, van de voormelde wet van 7 april 2019” opgeheven;

3° in hetzelfde lid worden de woorden “, aanbieder van essentiële diensten of digitaledienstverlener” opgeheven;

4° in hetzelfde lid worden de woorden “of de voormelde wet van 7 april 2019” opgeheven;

5° in het tweede lid, in de bepaling onder 2° worden de woorden “, de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” opgeheven;

Art. 54. In artikel 36, § 1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 4° worden de woorden “de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, §§ 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare

Art. 52. À l’article 16, § 4, de la même loi, les modifications suivantes sont apportées:

1° dans le premier alinéa, les mots “article 13 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “article 18 de la loi du [date] relative à la résilience des entités critiques”;

2° dans l’alinéa, les mots “articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 précitée” sont remplacés par les mots “articles 3, 2° et 31 de la loi du [date] précitée”;

3° dans le premier alinéa, les mots “des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique et”, “et à l’article 7, §§ 3 et 5, de la loi précitée du 7 avril 2019”, “, d’un opérateur de services essentiels ou d’un fournisseur de service numérique” et “ou de la loi précitée du 7 avril 2019” sont abrogés;

4° dans le deuxième alinéa, les mots “infrastructures critiques” sont remplacés par les mots “entités critiques”;

5° dans le deuxième alinéa, le 2° est remplacé par ce qui suit: “la loi du [date] relative à la résilience des entités critiques”;

Art. 53. À l’article 17, § 3, de la même loi, les modifications suivantes sont apportées:

1° dans l’alinéa 1er, les mots “et des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont abrogés;

2° dans le même alinéa, les mots “et à l’article 7, §§ 3 et 5, de la loi précitée du 7 avril 2019” sont abrogés;

3° dans le même alinéa, les mots “, d’un opérateur de services essentiels ou d’un fournisseur de service numérique” sont abrogés;

4° dans le même alinéa, les mots “ou de la loi précitée du 7 avril 2019” sont abrogés

5° dans le deuxième alinéa, le 2°, les mots “, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont abrogés.

Art. 54. À l’article 36, § 1er, de la même loi, les modifications suivantes sont apportées:

1° dans le4°, les mots “articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, à l’article 7, §§ 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont remplacés par les mots “articles 3, 2° et 31, de

veiligheid" vervangen door de woorden "de artikelen 3, 2° en 31, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten of de artikel 15, § 2, van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

2° in de bepaling onder 4° worden de woorden "en 15, §§ 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" opgeheven;

3° in de bepaling onder 4° worden de woorden "in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, van de voormelde wet van 7 april 2019" vervangen door de woorden "in artikelen 15, § 2, en 24 van de voormelde wet van […]".

Afdeling 4. Wijziging van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 55. In artikel 14 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, laatstelijk gewijzigd bij wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de volgende wijzigingen aangebracht:

a) in de eerste zin worden de woorden "met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "met betrekking tot de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, in de zin van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

b) in de bepaling onder 3°, wordt de bepaling onder g) vervangen als volgt:

"de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten, wat de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, betreft;

2° de bepaling onder 7° in paragraaf 2, eerste lid, wordt opgeheven.

Afdeling 5. Wijziging van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 56. In artikel 36/14 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, worden in de bepaling onder 20° de woorden "artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren zulks vereist" vervangen door de woorden "artikel 24 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten zulks vereist".

la loi du [date] relative à la résilience des entités critiques ou à l'article 15, § 2, de la loi du […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique";

2° dans le 4°, les mots "en 15, §§ 1 à 3, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien" sont abrogés;

3° dans le 4°, les mots "aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, de la loi précitée du 7 avril 2019" sont remplacés par les mots "aux articles 15, § 2, et 24 de la loi précitée du […]".

Section 4. Modification de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications

Art. 55. À l'article 14, de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications, modifiée en dernier lieu par la loi du 20 juillet 2022,les modifications suivantes sont apportées:

1° au paragraphe 1er, premier alinéa, les modifications suivantes sont apportées:

a) dans la première phrase, les mots "relevant des secteurs des communications électroniques et des infrastructures numériques aux sens de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "relevant du secteur des infrastructures numériques, à l'exception des fournisseurs de services de confiance, au sens de la loi du [date] relative à la résilience des entités critiques";

b) dans la disposition sous 3°, la dispositions sous g) est remplacée comme suit:

"la loi du [date] relative à la résilience des entités critiques, en ce qui concerne le secteur de l'infrastructure numérique, à l'exception des fournisseurs de services de confiance";

2° la disposition prévue au paragraphe 2, point 1, sous 7° est abrogée.

Section 5. Modification de la loi du 22 février 1998 portant le statut organique de la Banque nationale de Belgique

Art. 56. À l'article 36/14 de la loi du 22 février 1998 portant statut organique de la Banque nationale de Belgique, dans la disposition du 20°, les mots "l'article 19 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques l'exige" sont remplacés par les mots "l'article 24 de la loi du [date] relative à la résilience des entités critiques l'exige".

Art. 57. In artikel 36/49 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “kritieke infrastructuur” worden vervangen door de woorden “kritieke entiteit”;

2° de woorden “wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren” worden vervangen door de woorden “wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 6. Wijziging van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen

Art. 58. In artikel 15/2*sexies*, § 3, van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 4° worden de woorden “kritieke nationale infrastructuur” vervangen door de woorden “kritieke entiteit”;

2° in de bepaling onder 4° worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 7. Wijziging van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt

Art. 59. In artikel 14/1, § 3, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 4° worden de woorden “kritieke nationale infrastructuur” vervangen door de woorden “kritieke entiteit”;

2° in de bepaling onder 4° worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 8. Wijziging van het Strafwetboek

Art. 60 In artikel 546/2, § 1, van het Strafwetboek, ingevoegd bij wet van 20 mei 2016, wordt de bepaling onder 6° vervangen als volgt:

“6° Indien een kritieke entiteit, in de zin van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten werd binnengegaan of binnengedrongen”.

Art. 61. In artikel 550*ter*, § 1, van het Strafwetboek, ingevoegd bij wet van 28 november 2000 en gewijzigd bij de wet van 6 juli 2017, wordt het derde lid vervangen als volgt:

Art. 57. À l’article 36/49 de la même loi, les modifications suivantes sont apportées:

1° les mots “infrastructure critique” sont remplacés par les mots “entité critique”;

2° les mots “loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “loi du [date] relative à la résilience des entités critiques”.

Section 6. Modification de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations

Art. 58. À l’article 15/2*sexies*, § 3, de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, modifiée en dernier lieu par la loi du 31 juillet 2017, sont apportées les modifications suivantes:

1° dans la disposition sous 4°, les mots “infrastructure nationale critique” sont remplacés par les mots “entité critique”;

2° dans la disposition sous 4°, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du [date] relative à la résilience des entités critiques”.

Section 7. Modification de la loi du 29 avril 1999 relative à l’organisation du marché de l’électricité

Art. 59. À l’article 14/1, § 3, de la loi du 29 avril 1999 relative à l’organisation du marché de l’électricité, modifiée en dernier lieu par la loi du 31 juillet 2017, sont apportées les modifications suivantes:

1° dans la disposition sous 4°, les mots “infrastructure nationale critique” sont remplacés par les mots “entité critique”;

2° dans la disposition sous 4°, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du [date] relative à la résilience des entités critiques”.

Section 8. Modification du Code Pénal

Art. 60. À l’article 546/2, § 1er, du Code pénal, inséré par la loi du 20 mai 2016, la disposition sous 6° est remplacée comme suit:

“6° Si une entité critique, au sens de la loi du [date] sur la résilience des entités critiques, a fait l’objet d’une entrée ou d’une intrusion”.

Art. 61. À l’article 550*ter*, § 1er, du Code pénal, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juillet 2017, le troisième alinéa est remplacé comme suit:

"Dezelfde straf wordt toegepast wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt tegen een informatiesysteem van een kritieke entiteit zoals bedoeld in artikel 3, 3°, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 9. Wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 62. In artikel 15*bis*, lid 1, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, ingevoegd door de wet van 7 april 2019, worden de volgende wijzigingen aangebracht:

1°) de woorden "artikel 24 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren" worden vervangen door de woorden "artikel 31 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

2°) de woorden "aangeduid als kritieke infrastructuur krachtens bovengenoemde wet van 1 juli 2011" worden vervangen door de woorden "aangeduid als kritieke entiteit krachtens de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 10. Wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging

Art. 63. In artikel 6, § 1, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, gewijzigd bij de wet van 31 mei 2022, wordt een derde lid als volgt ingevoegd:

"Onverminderd de verplichtingen die zijn vastgelegd in de internationale instrumenten waardoor zij gebonden zijn, zijn de ondersteunende diensten verplicht om ambtshalve of op verzoek van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en de informatie waarover zij beschikken in het kader van hun wettelijke opdrachten en die relevant blijkt met het oog op de verwezenlijking van de doelstellingen van de dreigingsanalyse als bedoeld in artikel 8, § 2, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten, te communiceren."

Afdeling 11. Wijziging van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Art. 64. In artikel 3, § 4, van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid worden de woorden "exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren"

"La même peine est appliquée lorsque l'infraction visée à l'alinéa 1er est commise à l'encontre d'un système d'information d'une entité critique telle que visée à l'article 3, 3°, de la loi du [date] relative à la résilience des entités critiques".

Section 9. Modification de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 62. À l'article 15*bis*, alinéa 1, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, inséré par la loi du 7 avril 2019, les modifications suivantes sont apportées:

1°) les mots "l'article 24 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "l'article 31 de la loi du [date] relative à la résilience des entités critiques";

2°) les mots "désignés comme infrastructure critique en vertu de la loi du 1er juillet 2011 susmentionnée" sont remplacés par les mots "désignés comme entité critique en vertu de la loi du [date] relative à la résilience des entités critiques".

Section 10. Modification de la loi du 10 juillet 2006 relative à l'analyse de la menace

Art. 63. À l'article 6, § 1er de la loi du 10 juillet 2006 relative à l'analyse de la menace, modifié par la loi du 31 mai 2022, est inséré un alinéa 3 rédigé comme suit:

"Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'article 8, § 2, de la loi du [date] relative à la résilience des entités critiques."

Section 11. Modification de la loi du […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Art. 64. Dans l'article 3, § 4, de la loi du […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les mots "exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques" sont remplacés par les mots "entités

vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van […] betreffende de weerbaarheid van kritieke entiteiten”.

Art. 65. In artikel 8 van dezelfde wet wordt 43° vervangen door:

“43° “wet van [xx xxxx xxxx]”: de wet van […] betreffende de weerbaarheid van kritieke entiteiten”.

Art. 66. In artikel 15, § 2, tweede lid, van dezelfde wet worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van [xx xxxx xxxx]”.

Art. 67. In artikel 25 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in paragraaf 2 worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van [xx xxxx xxxx]”;

2° in paragraaf 4 wordt “wet van 1 juli 2011” vervangen door “wet van [xx xxxx xxxx]”;

3° in dezelfde paragraaf worden de woorden “exploitanten van infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt” vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]”.

Art. 68. In artikel 28, § 2, 7°, van dezelfde wet worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van [xx xxxx xxxx]”.

Art. 69. In artikel 37, § 5, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “wet van 1 juli 2011” worden vervangen door de woorden “wet van [xx xxxx xxxx]”;

2° de woorden “exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt” worden vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]”.

Art. 70. In artikel 40, § 1, tweede lid, van dezelfde wet worden de woorden “exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011” vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]”.

Art. 71. In artikel 45, § 1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “dat een exploitant van een infrastructuur die op grond van de wet van 1 juli 2011 als kritieke infrastructuur wordt aangemerkt” worden vervangen door de woorden “dat een kritieke entiteit als bedoeld in de wet van [xx xxxx xxxx]”;

2° de woorden “een exploitant van een infrastructuur die is aangemerkt als kritieke infrastructuur uit hoofde van de wet van

critiques au sens de la loi du […] relative à la résilience des entités critiques”.

Art. 65. Dans l’article 8 de la même loi, le 43° est remplacé par ce qui suit:

“43° “loi du [xx xxxx xxxx]”: la loi du […] relative à la résilience des entités critiques”.

Art. 66. Dans l’article 15, § 2, alinéa 2, de la même loi, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du [xx xxxx xxxx]”.

Art. 67. À l’article 25 de la même loi, les modifications suivantes sont apportées:

1° dans le paragraphe 2, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du [xx xxxx xxxx]”;

2° dans le paragraphe 4, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du [xx xxxx xxxx]”;

3° dans le même paragraphe, les mots “exploitants d’infrastructures recensées en tant qu’infrastructures critiques en vertu de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du [xx xxxx xxxx].

Art. 68. Dans l’article 28, § 2, 7°, de la même loi, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du [xx xxxx xxxx]”.

Art. 69. À l’article 37, § 5, de la même loi, les modifications suivantes sont apportées:

1° les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du [xx xxxx xxxx]”;

2° les mots “exploitants d’infrastructures identifiées comme infrastructures critique en vertu de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du [xx xxxx xxxx].

Art. 70. Dans l’article 40, § 1er, alinéa 2, de la même loi, les mots “exploitants d’une infrastructure critique au sens de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du [xx xxxx xxxx].

Art. 71. À l’article 45, § 1er, de la même loi, les modifications suivantes sont apportées:

1° les mots “qu’un exploitant d’une infrastructure définie comme critique en vertu de la loi du 1er juillet 2011” sont remplacé par les mots “qu’une entité critique au sens de la loi du [xx xxxx xxxx]”;

2° les mots “d’un exploitant d’une infrastructure qui est définie comme infrastructure critique en vertu de la loi du

1 juli 2011" worden vervangen door de woorden "een kritieke entiteit als bedoeld in de wet van [xx xxxx xxxx]";

3° de woorden "wet van 1 juli 2011" worden telkens vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 72. In artikel 67, 5°, van dezelfde wet worden de woorden "wet van 1 juli 2011" telkens vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 73. In artikel 68, 5°, van dezelfde wet worden de woorden "wet van 1 juli 2011" vervangen door de woorden "wet van [xx xxxx xxxx]".

HOOFDSTUK 10 – Slotbepalingen

Art. 74. De Koning neemt, bij een in Ministerraad overlegd besluit, de nodige maatregelen, met inbegrip van de opheffing, de aanvulling, de wijziging of de vervanging van wetsbepalingen, om de omzetting van de Europese richtlijnen betreffende de kritieke entiteiten te verzekeren.

Hij kan, bij een in Ministerraad overlegd besluit, de bepalingen van Hoofdstukken 4 tot en met 7 en de uitvoeringsbesluiten ervan volledig of gedeeltelijk van toepassing maken op andere sectoren dan diegene bedoeld in de Bijlage.

Art. 75. De wet van 1 juli 2011 betreffende de bescherming en beveiliging van kritieke infrastructuren wordt opgeheven.

Art. 76. § 1. Entiteiten die op grond van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren werden aangeduid als exploitanten van een Europese of nationale kritieke infrastructuur, worden op 17 juli 2026 van rechtswege beschouwd als kritieke entiteiten zoals bedoeld in artikel 12 van deze wet.

De lijst van kritieke infrastructuren zoals opgesteld volgens de wet van 1 juli 2011 zal, behoudens aanpassingen, voldoen aan artikel 12 van deze wet.

§ 2. De entiteiten bedoeld in paragraaf 1, lid 1, blijven tot 17 mei 2027 gehouden aan de verplichtingen uit de artikelen 13, 13/1, 13/2, 14, 24 en 25 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren, zoals deze op dat ogenblik van toepassing waren.

Art. 77. Met uitzondering van sectoren waarin nog geen kritieke entiteiten waren aangewezen voor de inwerkingtreding van deze wet, worden alle dreigingsanalyses geacht geldig te zijn voor een periode van maximaal vier jaar, overeenkomstig artikel 8, zelfs indien de datum waarop zij werden uitgevoerd voor de inwerkingtreding van deze wet valt.

Art. 78. Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

1er juillet 2011" sont remplacé par les mots "d'une entité critique au sens de la loi du [xx xxxx xxxx]";

3° les mots "loi du 1er juillet 2011" sont à chaque fois remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 72. Dans l'article 67, 5°, de la même loi, les mots "loi du 1er juillet 2011" sont à chaque fois remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 73. Dans l'article 68, 5°, de la même loi, les mots "loi du 1er juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]".

CHAPITRE 10 – Dispositions finales

Art. 74. Le Roi prend, par arrêté délibéré en Conseil des ministres, les mesures nécessaires, y compris l'abrogation, l'ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition des directives européennes concernant les entités critiques.

Il peut, par arrêté délibéré en Conseil des ministres, rendre applicables en tout ou en partie les dispositions des Chapitres 4 à 7 inclus et les arrêtés d'exécution à d'autres secteurs que ceux visés en Annexe.

Art. 75. La loi du 1er juillet 2011 relative à la protection et à la sécurité des infrastructures critiques est abrogée.

Art. 76. § 1er. Les entités qui ont été désignées comme exploitants d'une infrastructure critique européenne ou nationale en vertu de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques seront automatiquement considérées le 17 juillet 2026 comme des entités critiques au sens de l'article 12 de la présente loi.

La liste des infrastructures critiques telle qu'établie par la loi du 1er juillet 2011 sera conforme à l'article 12 de cette loi, sous réserve d'adaptations.

§ 2. Les entités visées au paragraphe 1, alinéa 1 restent tenues par les obligations énoncées aux articles 13, 13/1, 13/2, 14, 24 et 25 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques jusqu'au 17 mai 2027, telles qu'applicables à ce moment-là.

Art. 77. À l'exception des secteurs dans lesquels aucune entité critique n'avait encore été désignée avant l'entrée en vigueur de la présente loi, toutes les analyses de la menace sont réputées valables pendant une durée maximale de quatre ans, en vertu de l'article 8 et cela, même si la date à laquelle elles sont été effectuées est antérieure à l'entrée en vigueur de la présente loi.

Art. 78. La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

BIJLAGE

Sector	**Deelsector**	**Categorie van entiteit**	**Sectorale overheid**
1. Energie	Elektriciteit	Elektriciteitsbedrijven als bedoeld in art. 2, punt 57, van Richtlijn (EU) 2019/944, die de taak van "levering" in de zin van artikel 2, punt 12, van die richtlijn verrichten	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Distributiesysteembeheerders als bedoeld in art. 2, punt 29, van Richtlijn (EU) 2019/944	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 35, van Richtlijn (EU) 2019/944	
		Producenten als bedoeld in art. 2, punt 38, van Richtlijn (EU) nr. 2019/944	
		Benoemde elektriciteitsmarktbeheerders als bedoeld in art. 2, punt 8, van Verordening (EU) 2019/943	
		Op de elektriciteitsmarkt actieve marktdeelnemer als bedoeld in art. 2, punt 25, van Verordening (EU) 2019/943, die diensten verleent op het gebied van aggregatie, vraagrespons of energieopslag als bedoeld in art. 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944	
	Aardolie	Exploitanten van oliepijpleidingen	
		Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport	
		Centrale entiteiten voor de voorraadvorming als bedoeld in art. 2, punt f), van Richtlijn 2009/119/EG	
	Aardgas	Leveringsbedrijven als bedoeld in art. 2, punt 8, van Richtlijn 2009/73/EG	
		Distributiesysteembeheerders als bedoeld in art. 2, punt 6, van Richtlijn 2009/73/EG	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 4, van Richtlijn 2009/73/EG	
		Opslagsysteembeheerders als bedoeld in art. 2, punt 10, van Richtlijn 2009/73/EG	
		LNG-systeembeheerders als bedoeld in art. 2, punt 12, van Richtlijn 2009/73/EG	
		Aardgasbedrijven als bedoeld in art. 2, punt 1, van Richtlijn 2009/73/EG	
		Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas	
	Stadsverwarming- en koeling	Stadsverwarming en -koeling als bedoeld in art. 2, punt 19, van Richtlijn (EU) 2018/2001 ter bevordering van het gebruik van energie uit hernieuwbare bronnen	

	Waterstof	Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof	
2. Vervoer	Lucht	Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) 300/2008, die voor commerciële doeleinden worden gebruikt	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, Richtlijn 2009/12/EG van het Europees Parlement en de Raad, luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, Afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad zijn opgenomen, alsook de entiteiten die bijhorende installaties bedienen welke zich op de luchthavens bevinden	
		Luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad	
	Spoor	Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, Richtlijn 2012/34/EU van het Europees Parlement en de Raad	
		Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2012/34/EU, en exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die Richtlijn	
	Water	Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht zoals gedefinieerd in bijlage I bij Verordening (EG) 725/2004, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen	
		Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2005/65/EG, incl. hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, Verordening (EG) 725/2004, alsook entiteiten die werken en uitrusting in havens beheren	
		Exploitanten van verkeersbegeleiding-systemen zoals gedefinieerd in artikel 3, punt o), Richtlijn 2002/59/EG van het Europees Parlement en de Raad	
	Weg	Beheerders van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1 van Richtlijn 2010/40/EU van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, Verordening (EU) 2015/962 van de Commissie die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties voor wie verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteiten is	
	Openbaar vervoer	Openbaar vervoer exploitanten van diensten zoals gedefinieerd in artikel 2, punt d), Verordening (EG) 1370/2007 van het Europees Parlement en de Raad, met uitzondering van de entiteiten die reeds door een andere deelsector gevat worden	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
3. Bankwezen		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) 575/2013	**De Nationale Bank van België (NBB)**

4. Infrastructuur voor de financiële markt		Centrale tegenpartijen (CTP's) zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) 648/2012	**De Nationale Bank van België (NBB)**
		Beheerders van handelsplatforms zoals gedefinieerd in artikel 4, punt 24, Richtlijn 2014/65/EU	**De Autoriteit voor Financiële Diensten en Markten (FSMA)**
5. Digitale infrastructuur		Aanbieders van internetknooppunten zoals gedefinieerd in artikel 6, punt 18 van Richtlijn (EU) 2022/2555	**Het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.)**
		DNS-dienstverleners zoals gedefinieerd in artikel 6, punt 20, van Richtlijn (EU) 2022/2555, met uitzondering van exploitanten van root-naamservers	
		Registers voor topleveldomeinnamen zoals gedefinieerd in artikel 6, punt 21 van Richtlijn (EU) 2022/2555	
		Aanbieders van openbare elektronische-communicatienetwerken zoals gedefinieerd in art. 2, punt 8, van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad	
		Aanbieders van elektronische-communicatiediensten als bedoeld in art. 2, punt 4, van Richtlijn (EU) 2018/1972, voor zover hun diensten publiek beschikbaar zijn.	
		Aanbieders van netwerken voor *content delivery* zoals gedefinieerd in artikel 6, punt 32, van Richtlijn 2022/2555	
		Aanbieders van datacentrumdiensten zoals gedefinieerd in artikel 6, punt 31, van richtlijn 2022/2555	
		Aanbieders van cloudcomputingdiensten zoals gedefinieerd in artikel 6, punt 30, van Richtlijn 2022/2555	
		Verleners van vertrouwensdiensten zoals gedefinieerd in artikel 3, punt 19, van Verordening (EU) 910/2014 van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in art. 2, punt 1, a), Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad, maar met uitzondering van distributeurs voor wie de distributie van water voor menselijke consumptie slechts een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen	**De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
7. Afvalwater		Ondernemingen die stedelijk, huishoudelijk en industrieel afvalwater zoals gedefinieerd in art. 2, punten 1, 2 en 3, Richtlijn 91/271/EEG van de Raad opvangen, lozen of behandelen, met uitzondering van ondernemingen voor wie het opvangen, lozen of behandelen van stedelijk, huishoudelijk en industrieel afvalwater slechts een niet essentieel onderdeel van hun algemene activiteit is	**De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
8. Gezondheidszorg		Zorgaanbieders zoals gedefinieerd in art. 3, punt g), Richtlijn 2011/24/EG van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**

		EU-referentielaboratoria zoals gedefinieerd in art. 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad	**De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Entiteiten die zich bezighouden met onderzoek en ontwikkeling van geneesmiddelen zoals gedefinieerd in art. 1, punt 2, Richtlijn 2001/83/EG van het Europees Parlement en de Raad	**Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG)**
		Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen zoals gedefinieerd in sectie C, afd. 21, van NACE rev. 2 vervaardigen	
		Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (" de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") zoals gedefinieerd in art. 22 Verordening (EU) 2022/123 van het Europees Parlement en de Raad	
		Entiteiten met een distributievergunning zoals gedefinieerd in art. 79 Richtlijn 2001/83/EG	
9. Overheids		Overheidsinstanties van federale regeringen, met uitzondering van de rechterlijke macht, parlementen en centrale banken	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
10. Ruimtevaart		Exploitanten van grondfaciliteiten die in het bezit zijn van en beheerd en geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatie netwerken zoals gedefinieerd in art. 2, punt 8 Richtlijn (EU) 2018/1972	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
11. Productie, verwerking en distributie van levensmiddelen		Voedingsbedrijven zoals gedefinieerd in punt 2) van artikel 3 van Verordening (EG) nr. 178/20021 van het Europees Parlement en de Raad die zich uitsluitend bezighouden met logistiek en groothandelsdistributie en industriële productie op grote schaal en de verwerking ervan	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**

ANNEXE

Sector	**Sous-secteur**	**Catégorie d'entité**	**Autorité sectorielle**
1. Énergie	Électricité	Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/94445 du Parlement européen et du Conseil, qui assurent la fonction de "fourniture" au sens de l'article 2, point 12), de ladite directive	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944	
		Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944	
		Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944	
		Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil	
		Acteurs du marché de l'électricité au sens de l'article 2, point 25), du règlement (UE) 2019/943, qui fournit des services en matière d'agrégation, de participation active de la demande ou de stockage de l'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944	
	Pétrole	Exploitants d'oléoducs	
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole	
		Entités centrales de stockage de pétrole au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil	
	Gaz	Entreprises de fourniture au sens de l'article 2, point 8), de la directive 2009/73/CE du Parlement européen et du Conseil	
		Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE	
		Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE	
		Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la directive 2009/73/CE	
		Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE	
		Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE	
		Exploitants d'installations de raffinage et de traitement de gaz naturel	

	Réseaux de chaleur et de froid	Réseaux de chaleur ou de froid au sens de l'article 2, point 19), de la directive (UE) 2018/200147 du Parlement européen et du Conseil	
	Hydrogène	Exploitants d'installations de production, de stockage et de transport d'hydrogène	
2. Transports	Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 utilisés à des fins commerciales	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du conseil, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports	
		Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil	
	Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil	
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, et exploitants d'installations de services au sens de l'article 3, point 12), de ladite directive	
	Transports par eau	Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'Annexe I du règlement (CE) n° 725/2004, à l'exclusion des navires exploités à titre individuel par ces sociétés	
		Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE56, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports	
		Exploitants de services de trafic maritime au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil	
	Transports routiers	Systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
		Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de gestion du trafic, à l'exclusion des entités publiques pour lesquelles la gestion du trafic ou l'utilisation des systèmes de transport intelligents ne constituent qu'une partie non essentielle de leur activité générale	
	Transport public	Exploitants de services de transport public au sens de l'article 2 point (d) du règlement (CE) n° 1370/2007 du Parlement européen et du Conseil, à l'exception des entités qui relèvent déjà d'un autre sous-secteur	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil	**La Banque nationale de Belgique (BNB)**

4. Infrastructures de marchés financiers		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012	**La Banque nationale de Belgique (BNB)**
		Opérateurs de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE	**L'autorité des services et marchés financiers (FSMA)**
5. Infrastructures numériques		Fournisseurs de points d'échange internet au sens de l'article 6, point 18), de la directive (UE) 2022/2555	**Institut belge des services postaux et des télécommunications (I.B.P.T.)**
		Fournisseurs de services DNS au sens de l'article 6, point 20), de la directive (UE) 2022/2555, à l'exclusion des opérateurs de serveurs racines de noms de domaines	
		Registres de noms de domaines de premier niveau au sens de l'article 6, point 21), de la directive (UE) 2022/2555	
		Fournisseurs de services de centre de données au sens de l'article 6, point 31), de la directive (UE) 2022/2555	
		Fournisseurs de réseaux de diffusion de contenu au sens de l'article 6, point 32), de la directive (UE) 2022/2555	
		Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972 du Parlement européen et du Conseil	
		Fournisseurs de services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 dans la mesure où leurs services sont accessibles au public	
		Fournisseurs de services d'informatique en nuage au sens de l'article 6, point 30), de la directive (UE) 2022/2555	
		Prestataires de services de confiance au sens de l'article 3, point 19), du règlement (UE) n° 910/2014 du Parlement européen et du conseil	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie non essentielle de leur activité générale de distribution d'autres produits et biens	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
7. Eaux résiduaires		Entreprises assurant la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées et des eaux industrielles usées au sens de l'article 2, points 1) à 3), de la directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'élimination ou le traitement des eaux urbaines, ménagères et industrielles usées ne constituent qu'une partie non essentielle de leur activité générale	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
8. Santé		Prestataire de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
		Laboratoires de référence de l'Union européenne au sens l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du conseil	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**

		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil	**Agence fédérale des médicaments et des produits de santé (A.F.M.P.S.)**
		Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la section C, division 21, de la NACE Rév. 2	
		Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique ("liste des dispositifs médicaux critiques en cas d'urgence de santé publique") au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil	
		Entités titulaires d'une autorisation de distribution au sens de l'article 79 de la directive 2001/83/CE	
9. Administrations publiques		Administrations publiques du niveau fédéral,– excluant le pouvoir juridique, les parlements, et les banques centrales	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
10. Espace		Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**
11. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3 point 2 du règlement (CE) n°178/2021 du Parlement européen et du Conseil impliquées exclusivement dans la logistique et la distribution en gros et la production et la transformation à grande échelle	**L'autorité désignée par le Roi par arrêté pris en Conseil des ministres**

ADVIES VAN DE RAAD VAN STATE NR. 76.573/2/V VAN 12 AUGUSTUS 2024

Op 24 mei 2024 is de Raad van State, afdeling Wetgeving, door de Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing verzocht binnen een termijn van zestig dagen een advies te verstrekken over een voorontwerp van wet 'betreffende de weerbaarheid van kritieke entiteiten'.

Het voorontwerp is door de tweede vakantiekamer onderzocht op 29 juli 2024. De kamer was samengesteld uit Patrick Ronvaux, kamervoorzitter, Christine Horevoets en Laurence Vancrayebeck, staatsraden, en Béatrice Drapier, griffier.

Het verslag is uitgebracht door Roger Wimmer, eerste auditeur, en Benoît Lagasse, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre-Olivier de Broux, staatsraad.

Het advies, waarvan de tekst hierna volgt, is gegeven op 12 augustus 2024.

*

Aangezien de adviesaanvraag is ingediend op basis van artikel 84, § 1, eerste lid, 1°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,‡ de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

Voorafgaande vormvereisten

1. Het voorliggende voorontwerp, en inzonderheid de artikelen 23 tot 28, die immers voorzien in informatie-uitwisseling, impliceert de verwerking van persoonsgegevens in de zin van artikel 4, 1) en 2), van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)' (hierna: de "AVG").

‡ Aangezien het om amendementen op een wetsontwerp gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

AVIS DU CONSEIL D'ÉTAT N°76.573/2/V DU 12 AOÛT 2024

Le 24 mai 2024, le Conseil d'État, section de législation, a été invité par la Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique à communiquer un avis dans un délai de soixante jours, sur un avant-projet de loi 'concernant la résilience des entités critiques'.

L'avant-projet a été examiné par la deuxième chambre des vacations le 29 juillet 2024. La chambre était composée de Patrick Ronvaux, président de chambre, Christine Horevoets et Laurence Vancrayebeck, conseillers d'État, et Béatrice Drapier, greffier.

Le rapport a été présenté par Roger Wimmer, premier auditeur, et Benoît Lagasse, auditeur adjoint.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre-Olivier de Broux, conseiller d'État.

L'avis, dont le texte suit, a été donné le 12 août 2024.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 1°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet‡, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

Formalités préalables

1. L'avant-projet à l'examen, notamment ses articles 23 à 28, en ce qu'ils prévoient des échanges d'information, implique des traitements de données à caractère personnel au sens de l'article 4, 1) et 2), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)' (ci-après: le "RGPD").

‡ S'agissant d'amendements à un projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

Krachtens artikel 36, lid 4, van de AVG, gelezen in samenhang met artikel 57, lid 1, c), en met overweging 96 van de preambule, alsook in voorkomend geval met artikel 2, tweede lid, van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', dient de toezichthoudende autoriteit, in casu de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit', te worden geraadpleegd bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel, in verband met de verwerking van persoonsgegevens.

Bijgevolg moet het advies van de Gegevensbeschermingsautoriteit worden ingewonnen.

2. Bovendien bepaalt artikel 6, § 4, 3°, van de bijzondere wet van 8 augustus 1980 'tot hervorming der instellingen' dat de regeringen betrokken moeten worden bij "het ontwerpen van de regels van de algemene politie met uitzondering van de regels van politie over het verkeer op waterwegen bedoeld in § 1, X, 10°, en de reglementering op het verkeer en vervoer, alsook van de technische voorschriften inzake verkeers- en vervoermiddelen".

Aangezien het voorontwerp onder meer de vervoerssector beoogt, zijn de gewesten per brief van het voorontwerp op de hoogte gebracht en is hun gevraagd hun standpunt mee te delen binnen een termijn van zestig dagen. Bij de adviesaanvraag zijn kopieën gevoegd van die brieven, die net als de adviesaanvraag 23 mei 2024 gedateerd zijn.

Aangezien de Raad van State geadieerd is op 24 mei 2024, dient vastgesteld te worden dat het vormvereiste bedoeld in artikel 6, § 4, 3°, van de bijzondere wet van 8 augustus 1980, nog niet volledig vervuld is.

3. Indien de aan de Raad van State voorgelegde tekst naar aanleiding van het vervullen van die vormvereisten nog wijzigingen zou ondergaan die niet louter vormelijk zijn en niet voortvloeien uit het gevolg dat aan dit advies wordt gegeven, moeten de gewijzigde of toegevoegde bepalingen op hun beurt om advies aan de afdeling Wetgeving worden voorgelegd, overeenkomstig artikel 3, § 1, eerste lid, van de gecoördineerde wetten 'op de Raad van State'.

ALGEMENE OPMERKINGEN

I. Strekking van het voorontwerp

Het voorliggende voorontwerp strekt tot omzetting in Belgisch recht van richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 'betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad' (hierna: de "CER-richtlijn"), die tot doel heeft de weerbaarheid te verhogen van de kritieke entiteiten die essentiële diensten leveren op het vlak van vitale maatschappelijke functies of vitale economische activiteiten op de interne markt.

L'article 36, paragraphe 4, du RGPD, combiné avec son article 57, paragraphe 1, c), le considérant 96 de son préambule et, le cas échéant, l'article 2, alinéa 2, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', prévoit une obligation de consulter l'autorité de contrôle, en l'occurrence l'Autorité de protection des données visée dans la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement de données à caractère personnel.

Il s'impose par conséquent de recueillir l'avis de l'Autorité de protection des données.

2. Par ailleurs, l'article 6, § 4, 3°, de la loi spéciale du 8 août 1980 'de réformes institutionnelles' prévoit que les gouvernements seront associés "à l'élaboration des règles de police générale à l'exception des règles de police de la navigation sur les voies navigables visées au § 1er, X, 10°, et de la réglementation relatives aux communications et aux transports, ainsi qu'aux prescriptions techniques relatives aux moyens de communication et de transport".

Dans la mesure où l'avant-projet vise notamment le secteur des transports, la demande d'avis du 23 mai 2024 contient des courriers datés du même jour adressés aux différentes Régions les informant de l'avant-projet et leur demandant de communiquer leur point de vue dans un délai de soixante jours.

Étant donné que le Conseil d'État a été saisi le 24 mai 2024, il y a lieu de constater que la formalité prévue à l'article 6, § 4, 3°, de la loi spéciale du 8 août 1980 n'a pas encore été effectuée en totalité.

3. Si l'accomplissement de ces formalités devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme et ne résultant pas des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation conformément à l'article 3, § 1er, alinéa 1er, des lois coordonnées 'sur le Conseil d'État'.

OBSERVATIONS GÉNÉRALES

I. La portée de l'avant-projet

L'avant-projet examiné vise à transposer en droit belge la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 'sur la résilience des entités critiques et abrogeant la directive 2008/114/CE du Conseil' (ci-après: la "directive CER"), laquelle a pour objectif d'accroître la résilience des entités critiques qui fournissent des services essentiels pour les fonctions sociétales ou les activités économiques vitales dans le marché intérieur.

De CER-richtlijn strekt eveneens tot opheffing en vervanging van richtlijn 2008/114/EG van de Raad van 8 december 2008 'inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren' (hierna: de "ECI-richtlijn"). In de memorie van toelichting staat dat die richtlijn uitsluitend gericht was op de beveiliging van Europese kritieke infrastructuren in de sectoren energie en transport, waarvan de ontwrichting of vernietiging aanzienlijke grensoverschrijdende gevolgen zou hebben voor ten minste twee lidstaten.

Die richtlijn is omgezet in Belgisch recht bij de wet van 1 juli 2011 'betreffende de beveiliging en de bescherming van de kritieke infrastructuren', welke wet opgeheven wordt bij artikel 75 van het voorontwerp.

Terwijl in de ECI-richtlijn het begrip "kritieke infrastructuren" gebruikt werd, wordt in de CER-richtlijn hoofdzakelijk het concept "kritieke entiteiten" gehanteerd, ook al blijft het begrip "kritieke infrastructuren" nog behouden. Luidens de memorie van toelichting wordt een entiteit als kritiek beschouwd als ze voldoet aan drie voorwaarden: de entiteit verleent essentiële diensten, de kritieke infrastructuur bevindt zich op het Belgische grondgebied en een incident zou een aanzienlijk verstorend effect hebben op het verlenen van die essentiële diensten. De taak om te bepalen welke entiteiten kritieke entiteiten zijn, wordt toevertrouwd aan de sectorale overheden, te weten de overheden, aangewezen door de Koning met toepassing van artikel 21, § 4, van het voorontwerp, die bevoegd zijn voor een bepaalde sector of deelsector.

In de memorie van toelichting staat nog het volgende:

"Kritieke entiteiten spelen als verleners van essentiële diensten een onmisbare rol bij het in stand houden van vitale maatschappelijke functies of economische activiteiten op de interne markt, in een economie die in de Europese Unie in toenemende mate onderling afhankelijk is. Het wetsontwerp heeft als doel te waken over het behoud en de weerbaarheid van vitale functies zoals onder andere de productie en transport van energie, de vitale vervoersinfrastructuren en -systemen, de onontbeerlijke schakels in het elektronische betalingsvervoer, de vitale verbindingen van elektronische communicatie. de onmisbare entiteiten in de gezondheidszorg en faciliteiten die ervoor zorgen dat burgers over drinkwater beschikken. Het wetsontwerp stelt een gemeenschappelijke benadering in werking waarbij rekening wordt gehouden met het essentiële karakter van de sectoren waarop de CER-Richtlijn wordt toegepast, met name de sectoren: energie, vervoer, bankwezen, financiële marktinfrastructuur, digitale infrastructuur, drinkwater, afvalwater, volksgezondheid, overheidsinstellingen, ruimtevaart en voeding.

Deze wetgeving situeert zich hoofdzakelijk in het domein van de preventie. Het gaat om de organisatie van het nemen van weerbaarheidsmaatregelen door de kritieke entiteit, en indien noodzakelijk beschermingsmaatregelen door de bevoegde overheden, teneinde elk voorval dat van aard is om een aanzienlijk verstorend effect te hebben op de verlening van essentiële diensten door de kritieke entiteit, te voorkomen

La directive CER vise également à abroger et remplacer la directive 2008/114/CE du Conseil du 8 décembre 2008 'concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection' (ci-après: la "directive ICE"). L'exposé des motifs précise que cette directive était exclusivement axée sur la protection des infrastructures critiques européennes dans les secteurs de l'énergie et des transports dont l'arrêt ou la destruction aurait un impact transfrontalier significatif pour au moins deux États membres.

Cette directive a été transposée en droit belge par la loi du 1er juillet 2011 'relative à la sécurité et la protection des infrastructures critiques', laquelle est abrogée par l'article 75 de l'avant-projet.

Alors que la directive ICE renvoyait à la notion d'infrastructures critiques, la directive CER a principalement recours au concept d'entités critiques, même si la notion d'infrastructures critiques est maintenue. Selon l'exposé des motifs, une entité critique est identifiée comme telle lorsqu'elle répond à trois conditions: l'entité fournit des services essentiels, l'infrastructure critique se situe sur le territoire belge et un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels. La mission d'identification des entités critiques est confiée aux autorités sectorielles, à savoir les autorités compétentes pour un secteur ou sous-secteur déterminé, désignées par le Roi, en application de l'article 21, § 4, de l'avant-projet.

On peut encore lire ce qui suit dans l'exposé des motifs:

"En tant que fournisseurs de services essentiels, les entités critiques jouent un rôle indispensable dans le maintien des fonctions sociétales ou des activités économiques vitales sur le marché intérieur, dans une économie de plus en plus interdépendante au sein de l'Union européenne. Le projet de loi vise à veiller au maintien et à la résilience des fonctions vitales, entre autres la production et le transport d'énergie, les points nodaux vitaux du transport, les maillons indispensables dans le transport des paiements électroniques, les connexions vitales de la communication électronique, les entités indispensables aux soins de santé et les installations qui permettent aux citoyens de disposer d'eau potable. Le projet met en place une approche commune qui tient compte du caractère essentiel des secteurs auxquels la directive CER s'applique, à savoir: l'énergie, les transports, le secteur bancaire, l'infrastructure des marchés financiers, l'infrastructure numérique, l'eau potable, les eaux usées, la santé publique, les institutions publiques, l'espace et l'alimentation.

Cette législation se situe principalement dans le domaine de la prévention. Il s'agit d'organiser la prise de mesures de résilience par l'entité critique et, si nécessaire, de mesures de protection par les autorités compétentes afin de prévenir ou empêcher tout événement de nature à perturber de manière significative la fourniture des services essentiels par l'entité critique. Au cas où un incident survient malgré tout, cette

of te verhinderen. In het geval een incident zich toch voordoet, poogt deze wetgeving de kritieke entiteiten de nodige tools te geven om zich hiertegen te verdedigen."

II. Het voorontwerp in het licht van de regels inzake bevoegdheidsverdeling

1. In de memorie van toelichting wordt opgemerkt dat de omzetting van de CER-richtlijn mogelijk een impact heeft op sectoren die onder de bevoegdheid van de deelstaten vallen. Het toepassingsgebied van het voorontwerp omvat immers een hele reeks sectoren, zoals die welke instaan voor de drinkwatervoorziening of de afvalwaterverwerking, waarvoor zowel de federale overheid als de deelstaten bevoegd zijn.

Volgens de steller valt het voorontwerp onder te brengen bij de residuaire bevoegdheid van de federale overheid inzake veiligheid en openbare orde, en meer bepaald inzake preventieve bescherming op het gebied van de openbare veiligheid.

In de memorie van toelichting wordt dat als volgt verduidelijkt:

"Naast de algemene preventieve bescherming van kritieke infrastructuren, is de federale overheid ook residuair bevoegd voor de strijd tegen radicalisme, extremisme, terrorisme en de bescherming van de infrastructuur tegen terroristische aanslagen (…) Het gaat om een algemene preventieve beschermingsbevoegdheid. De nieuwe CER-Richtlijn herneemt deze 'alle-risico's aanpak', zonder enige prioritering tussen de soorten dreigingen, aangezien er sprake is van een dynamisch dreigingslandschap. (…)

De in dit ontwerp te vinden evolutie van kritieke infrastructuur naar kritieke entiteit wijzigt niets aan de grondslag van de wetgeving. Deze blijft zich gronden in het gebied van de openbare veiligheid. Het doel van dit ontwerp is namelijk net om de bescherming en beveiliging van kritieke entiteiten te verhogen, en om deze entiteiten weerbaar te maken tegen alle mogelijke soorten risico's."

In advies 48.989/VR van 9 december 2010 over het voorontwerp van wet dat geleid heeft tot de wet van 1 juli 2011 heeft de afdeling Wetgeving het volgende opgemerkt:

"1. Het voorliggende voorontwerp voorziet, zoals te lezen staat in artikel 2, eerste lid, ervan, inzonderheid in de omzetting van richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (hierna 'de richtlijn' genoemd).

Artikel 1 van de richtlijn geeft aan dat bij deze richtlijn een procedure wordt ingesteld voor de identificatie en de aanmerking van Europese kritieke infrastructuren, om de bescherming van de mensen te bevorderen. De kritieke infrastructuur wordt in artikel 2, a), van de richtlijn in wezen gedefinieerd als 'een voorziening (…, die) van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk

législation tente de fournir aux entités critiques les outils nécessaires pour s'en protéger".

II. L'avant-projet au regard des règles de répartition des compétences

1. L'exposé des motifs relève qu'il est possible que la transposition de la directive CER ait un impact sur des secteurs relevant de la compétence des entités fédérées dans la mesure où le champ d'application de l'avant-projet englobe toute une série de secteurs comme celui de l'eau potable ou du traitement des eaux résiduaires pour lesquels la compétence est répartie entre les entités fédérale et fédérées.

L'auteure de l'avant-projet entend s'inscrire dans la compétence résiduelle de l'autorité fédérale en matière de sécurité et d'ordre public et, plus précisément, en matière de protection préventive dans le domaine de la sécurité publique.

L'exposé des motifs explicite comme suit cette intention:

"Outre la protection préventive générale des infrastructures critiques, le gouvernement fédéral dispose également d'une compétence résiduelle en matière de lutte contre le radicalisme, l'extrémisme, le terrorisme et la protection des infrastructures contre les attaques terroristes […] Il s'agit d'une compétence générale de protection préventive. La nouvelle Directive CER réaffirme cette 'approche tous risques', sans établir de priorités entre les types de menaces, étant donné que le paysage des menaces est dynamique. […].

L'évolution de la notion d'infrastructure critique à celle d'entité critique que l'on trouve dans le projet ne modifie pas la base de la législation. Celle-ci reste ancrée dans la sécurité publique. En effet, l'objectif de ce projet est précisément d'accroître la protection et la sécurité des entités critiques et de les rendre résistantes à toutes sortes de risques".

Dans l'avis 48.989/VR donné le 9 décembre 2010 sur l'avant-projet de loi devenu la loi du 1er juillet 2011, la section de législation a indiqué ce qui suit:

"1. Ainsi que l'exprime son article 2, alinéa 1er, l'avant-projet à l'examen a notamment pour objet de transposer la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (ci–après, la directive).

Comme l'énonce l'article 1er de la directive, il s'agit d'établir une procédure de recensement et de désignation des infrastructures critiques européennes en vue d'éventuellement améliorer leur protection afin de contribuer à la protection des personnes. L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme 'le point (…) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou

welzijn, waarvan de verstoring of vernietiging (…) aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken'. Artikel 3, lid 3, van de richtlijn bepaalt dat deze op dit ogenblik uitsluitend van toepassing is in de sectoren energie en vervoer. Volgens de eerste overweging van de richtlijn hebben de stellers ervan in de eerste plaats het aannemen van 'voorstellen (beoogd) over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur in Europa kunnen worden verbeterd'. In dat verband is besloten dat het Europese programma voor de bescherming van kritieke infrastructuren, waarvan de richtlijn een beleidsmiddel is, 'gebaseerd moet zijn op een alle risico's omvattende aanpak, waarbij de bestrijding van terroristische dreigingen als prioriteit zou gelden', een aanpak waarbij 'in het proces ter bescherming van kritieke infrastructuur rekening (dient) te worden gehouden met door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen' (derde overweging).

Gelet op hetgeen voorafgaat, moet worden beschouwd dat de omzetting van deze richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort.[1]

Hetzelfde geldt voor de overige bepalingen van het voorontwerp die weliswaar niet voorzien in de omzetting van de richtlijn, maar strekken tot het aannemen van analoge maatregelen met betrekking tot de nationale kritieke infrastructuren, de andere punten van federaal belang en de punten van lokaal belang.

2. De maatregelen die op basis van het voorontwerp zullen worden getroffen, kunnen evenwel een weerslag hebben op operatoren die een infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid ratione materiae van de gewesten kan behoren, meer in het bijzonder wat betreft de sectoren energie en vervoer, waarop de richtlijn toepassing vindt (artikel 6, § 1, VII en X, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen).

De steller van het voorontwerp heeft overigens oog gehad voor dit aspect, daar hij de gewesten wenst te 'betrekken' bij het uitwerken van de toepasselijke regelgeving en bij de uitvoering ervan, zoals blijkt uit de volgende bepalingen van het voorontwerp:

(…)

3. Aangezien de gewesten bevoegdheden bezitten op het gebied van energie en vervoer, aangezien dit eveneens zou

[1] *Voetnoot 1 van het geciteerde advies:* Raad van State, Belgische Staat, nr. 175.462, 8 oktober 2007. Andere voorbeelden van wetten die de Federale Staat heeft aangenomen met het oog op de preventieve bescherming van de "vitale maatschappelijke functies": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, die onder meer de bescherming van het "economisch potentieel van het land" beoogt, of de wet van 10 juli 2006 betreffende de analyse van de dreiging, die onder meer 's lands "fundamentele belangen" beoogt.

social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (…) du fait de la défaillance de ces fonctions'. L'article 3, paragraphe 3, de la directive mentionne qu'elle s'applique pour l'instant uniquement dans les secteurs de l'énergie et des transports. Selon le premier considérant de la directive, ses auteurs ont d'abord eu en vue l'adoption de 'mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques'. Par la suite, tout en maintenant 'une priorité donnée à la lutte contre la menace terroriste', le programme européen de protection des infrastructures critiques, dont la directive est un instrument, s'est fondé sur 'une approche tous risques (qui) tient compte des risques d'origine humaine, des menaces technologiques et des catastrophes naturelles dans le processus de protection des infrastructures critiques' (troisième considérant).

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral[1].

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local.

2. Toutefois, les mesures qui seront prises sur la base de l'avant-projet seront susceptibles de concerner des opérateurs exploitant des infrastructures qui, envisagées d'un autre point de vue, pourraient relever de la compétence matérielle des régions, s'agissant spécialement des secteurs de l'énergie et du transport, auxquels la directive s'applique (article 6, § 1er, VII et X, de la loi spéciale du 8 août 1980 de réformes institutionnelles).

L'auteur de l'avant-projet est d'ailleurs sensible à cet aspect des choses puisqu'il a le souci d''associer' les régions à la réglementation applicable et à sa mise en œuvre, comme en témoignent les dispositions suivantes de l'avant-projet:

[…]

3. Comme les régions détiennent des compétences dans les domaines de l'énergie et du transport, qu'il pourrait en

[1] *Note de bas de page n° 1 de l'avis cité:* C.E., État belge, n° 175.462, 8 octobre 2007. Pour d'autres exemples de lois adoptées par l'État fédéral en vue d'assurer la protection préventive des "fonctions vitales de la société", voir la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité qui vise notamment à protéger "le potentiel économique du pays" ou la loi du 10 juillet 2006 relative à l'analyse de la menace qui a notamment en vue les "intérêts fondamentaux" du pays.

kunnen gelden voor andere sectoren waarop de ontworpen wet toepassing zou vinden en volgens de steller zelf van het voorontwerp bij de uitvoering van de wet de weerslag van sommige van de voorgenomen maatregelen voelbaar zou kunnen zijn in het beheer van infrastructuren die tot de bevoegdheid van de gewesten behoren, kan worden aanvaard dat de gewesten worden betrokken bij het aannemen van de uitvoeringsmaatregelen omschreven in de ontworpen tekst.

De steller van het voorontwerp moet evenwel aldus te werk gaan dat de autonomie van de verschillende beleidsniveaus in acht wordt genomen. De federale wetgever kan niet eenzijdig - bij wege van een gewone wet - een gedwongen medewerking van de gewesten aan het bij het voorontwerp uitgestippelde systeem opleggen. De medewerking van de gewesten kan dus indien nodig alleen facultatief zijn, en op een zodanige wijze dat, indien ze dat verzuimen, zulks niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen kan nemen.

4. Indien in de toekomst mocht blijken dat het aannemen van maatregelen ter uitvoering van de wet inhoudt dat bevoegdheden eigen aan de federale overheid en aan de gewesten gezamenlijk worden uitgeoefend, en niet meer dat uitsluitend de enkele federale bevoegdheid op het gebied van de openbare veiligheid wordt uitgeoefend, moet daaromtrent met de gewesten een samenwerkingsakkoord worden gesloten."[2-3]

Onder voorbehoud van de opmerking gemaakt bij artikel 30, heeft de steller van het voorontwerp, in overeenstemming met die beginselen, in de voorgelegde tekst en meer bepaald in de artikelen 7, § 2, tweede lid, 9, § 1, derde lid, 10, § 2, eerste lid, 11, 12, § 1, derde lid, en 22, tweede lid, bepaald dat de deelstaten facultatief betrokken worden bij de ontworpen regelgeving.

In het licht van wat hierboven is uiteengezet, levert het voorontwerp dus geen bevoegdheidsproblemen op.

III. Het voorontwerp en de samenhang met de bestaande wet- en regelgeving

1. Zoals reeds opgemerkt, wil de steller van het voorontwerp de ontworpen wetgeving in het domein van de preventie situeren, aangezien de beschermingsmaatregelen die de bevoegde overheden nemen, erop gericht zijn elk voorval dat

[2] Advies 48.989/VR van 9 december 2010 over een voorontwerp dat geleid heeft tot de wet van 1 juli 2011 'betreffende de beveiliging en de bescherming van de kritieke infrastructuren' (*Parl.St.* Kamer 2010-11, nr. 53-1357/001, 53-55).

[3] Zie in dezelfde zin ook advies 68.936/AV van 7 april 2021 over een voorontwerp dat geleid heeft tot de wet van 14 augustus 2021 'betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie' (*Parl.St.* Kamer 2020-21, nr. 55-1951/001, 55 tot 127), advies 74.861/4 van 10 januari 2024 over een voorontwerp dat geleid heeft tot de wet van 26 april 2024 'tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' (*Parl.St.* Kamer 2023-24, nr. 55-3862/001, 161-176) en advies 76.050/2. In deze adviezen wordt verwezen naar advies 48.989/VR. Zie ook GwH 10 maart 2022, nr. 33/2022, B.13.1, en 22 september 2022, nr. 110/2022, B.11.2.

être de même pour d'autres secteurs auxquels la loi en projet s'appliquerait et que, selon l'auteur de l'avant-projet lui-même, dans l'exécution de la loi, l'incidence de certaines des mesures envisagées pourrait affecter la gestion d'infrastructures relevant des compétences régionales, il est admissible d'associer les régions à l'adoption des mesures d'exécution du texte en projet.

Toutefois, ce faisant, il doit le faire d'une manière qui respecte l'autonomie des différents niveaux de pouvoir. Le législateur fédéral ne peut imposer unilatéralement - par le biais d'une loi ordinaire - une collaboration forcée des régions au système mis en place par l'avant-projet. L'intervention des régions ne peut être prévue, si nécessaire, que de façon facultative et en manière telle que leur éventuelle abstention n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale compétente.

4. Si, dans l'avenir, il devait s'avérer que l'adoption des mesures d'exécution de la loi devait impliquer l'exercice conjoint de compétences propres à l'autorité fédérale et aux régions, et non plus uniquement la mise en œuvre de la seule compétence fédérale en matière de sécurité publique, il conviendrait de conclure un accord de coopération avec les régions sur ces questions"[2-3].

Sous la réserve de l'observation formulée sous l'article 30, c'est en conformité avec ces principes que l'auteure de l'avant-projet a prévu dans le texte soumis à l'examen et, plus précisément, aux articles 7, § 2, alinéa 2, 9, § 1er, alinéa 3, 10, § 2, alinéa 1er, 11, 12, § 1er, alinéa 3, et 22, alinéa 2, une association facultative des entités fédérées à la réglementation en projet.

Dans la mesure qui vient d'être exposée, l'avant-projet ne soulève donc pas de difficulté de compétence.

III. L'avant-projet et son articulation avec les dispositifs législatifs et réglementaires existants

1. Ainsi qu'il a été relevé, l'auteure de l'avant-projet entend situer la législation en projet dans le domaine de la prévention, les mesures de protection prises par les autorités compétentes visant à prévenir ou empêcher tout événement de nature à

[2] Avis 48.989/VR donné le 9 décembre 2010 sur un avant-projet devenu la loi du 1er juillet 2011 'relative à la sécurité et la protection des infrastructures critiques' (*Doc. parl.*, Chambre, 2010-2011, n° 53-1357/001, pp. 53-55).

[3] Dans le même sens, voir également l'avis 68.936/AG donné le 7 avril 2021 sur un avant-projet devenu la loi du 14 août 2021 'relative aux mesures de police administrative lors d'une situation d'urgence épidémique' (*Doc. parl.,* Chambre, 2020-2021, n° 55-1951/001, pp. 55 à 127), l'avis 74.861/4 donné le 10 janvier 2024 sur un avant-projet devenu la loi du 26 avril 2024 'établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique' (*Doc. parl.*, Chambre, 2023-2024, n° 55-3862/001, pp. 161-176) et l'avis 76.050/2, lesquels renvoient à l'avis 48.989/VR. Voir aussi C.C, 10 mars 2022, n° 33/2022, B.13.1 et 22 septembre 2022, n° 110/2022, B.11.2.

een aanzienlijk verstorend effect kan hebben op het verlenen van essentiële diensten door de betrokken kritieke entiteiten, te voorkomen of te verhinderen.

In de memorie van toelichting staat in dat verband dat het voorontwerp evenwel niet kadert in de voorbereiding van het beheer van een noodsituatie, aangezien in voorkomend geval de bestaande wet- en regelgeving moet worden toegepast. In dat verband wordt verwezen naar de wet van 31 december 1963 'betreffende de civiele bescherming', het koninklijk besluit van 31 januari 2003 'tot vaststelling van het noodplan voor de crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen', de wet van 15 mei 2007 'betreffende de civiele veiligheid' en het koninklijk besluit van 22 mei 2019 'betreffende de noodplanning en het beheer van noodsituaties op gemeentelijk en provinciaal niveau en betreffende de rol van de burgemeesters en de provinciegouverneurs in geval van crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen'.

De steller van het voorontwerp wordt er evenwel op gewezen dat de afdeling Wetgeving onlangs geadieerd is omtrent een voorontwerp van wet "betreffende noodplanning en crisisbeheer", waarover op 6 juni 2024 advies 76.050/2 gegeven is.

De afdeling Wetgeving heeft in dat advies opgemerkt dat

"het voorontwerp een specifiek juridisch kader moet ontwikkelen 'voor noodplanning en crisisbeheer', waarin de taken en verantwoordelijkheden van de verschillende actoren worden omschreven, met het oog op een optimale organisatie van het crisisbeheer en om de overgang van een sectoraal incident naar een nationale crisis te vergemakkelijken.

(…)

Wat betreft noodplanning en crisisbeheer op nationaal niveau, streeft het voorliggende voorontwerp naar een harmonisatie zodat nationale noodsituaties, ongeacht wat hun oorsprong is, vanaf het begin met dezelfde basisaanpak en -structuur worden beheerd. Dankzij de aldus ingevoerde automatismen zou men bij het begin van een crisis kostbare tijd kunnen besparen maar indien nodig ook meerdere gelijktijdige of onderling verbonden crisissen op gestructureerde wijze beheren."

De afdeling Wetgeving heeft vastgesteld dat evenwel niet tegemoetgekomen kon worden aan de nagestreefde harmonisering en verduidelijking indien het betreffende voorontwerp niet werd afgestemd op de bestaande wet- en regelgeving inzake planning, coördinatie en beheer van crisissen. Wat dat betreft, zijn meerdere lacunes blootgelegd, met name in verband met bepalingen die strekten tot wijziging van de wet van 31 december 1963, van de wet van 15 mei 2007 of van het koninklijk besluit van 22 mei 2019.

Zo ook moet de steller van het voorontwerp zich vergewissen van een goede samenhang tussen het voorliggende dispositief en het dispositief dat zou voortvloeien uit het voorontwerp dat

perturber de manière significative la fourniture de services essentiels par les entités critiques concernées.

L'exposé des motifs précise à cet égard que l'avant-projet ne se situe toutefois pas dans le cadre des préparatifs liés à la gestion d'une situation d'urgence, les dispositions légales et réglementaires existantes devant le cas échéant s'appliquer. Ainsi, sont cités la loi du 31 décembre 1963 'relative à la protection civile', l'arrêté royal du 31 janvier 2003 'portant fixation du plan d'urgence sur les événements et situations de crise nécessitant une coordination ou une gestion à 1'échelon national', la loi du 15 mai 2007 'relative à la sécurité civile' et l'arrêté royal du 22 mai 2019 'relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial et au rôle des bourgmestres et des gouverneurs de province en cas d'événements et de situations de crise nécessitant une coordination ou une gestion à 1'échelon national'.

L'attention de l'auteure de l'avant-projet est toutefois attirée sur le fait que la section de législation a récemment été saisie d'une demande d'avis sur un avant-projet de loi "relative à la planification d'urgence et à la gestion de crise" qui a donné lieu à l'avis 76.050/2 du 6 juin 2024.

Comme la section de législation l'a relevé dans cet avis,

"l'avant-projet est destiné à créer un cadre légal spécifique 'pour la planification d'urgence et la gestion de crise' qui permette de définir le rôle et les responsabilités des différents acteurs afin d'assurer, lorsque celle-ci survient, une gestion de crise optimale et de faciliter la transition d'un incident sectoriel vers une crise nationale.

[…]

Quant à la planification et à la gestion de crise au niveau national, l'avant-projet examiné poursuit un objectif d'harmonisation afin de gérer dès le départ les situations d'urgence d'ampleur nationale, quelle qu'en soit l'origine, selon la même approche et la même structure de base. Les automatismes qui seraient ainsi créés devraient permettre de gagner un temps précieux au début d'une crise mais aussi permettre le cas échéant de gérer de manière structurée plusieurs crises concomitantes ou interconnectées".

La section de législation a constaté que l'harmonisation et la clarification poursuivies ne pouvaient toutefois être rencontrées sans articuler l'avant-projet concerné avec les dispositifs législatifs et réglementaires existants en matière de planification, de coordination et de gestion de crise. Plusieurs lacunes avaient à cet égard été relevées, s'agissant notamment de dispositions tendant à modifier les lois du 31 décembre 1963 et du 15 mai 2007 ou l'arrêté royal du 22 mai 2019.

De la même manière, l'auteure de l'avant-projet s'assurera de la correcte articulation entre le dispositif examiné et celui qui adviendrait de l'avant-projet ayant donné lieu à l'avis 76.050/2,

aanleiding gegeven heeft tot advies 76.050/2, alsook tussen de wetgevende en verordeningsbepalingen die ten gevolge daarvan gewijzigd zouden worden.

De aandacht van de steller van het voorontwerp wordt meer in het bijzonder gevestigd op artikel 20 van het voorontwerp, dat een bijzondere procedure instelt "wanneer zich een gebeurtenis voordoet die van aard is om de verlening van essentiële diensten aanzienlijk te verstoren". Zodoende wordt bij artikel 20 niet langer de preventie van een incident geregeld maar wel het beheer ervan nadat het zich heeft voorgedaan, zodat de procedure in kwestie moet worden afgetoetst aan, en in voorkomend geval afgestemd op, de procedure die van toepassing is inzake crisisbeheer.

2. In dezelfde gedachtegang verwijst het voorontwerp meerdere keren naar andere wetgevingen, onder meer naar de wet van 11 december 1998 'betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst'.[4] Die wet is evenwel recent gewijzigd bij de wet van 2 juni 2024 'houdende wijziging van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', waarvan artikel 2, bijvoorbeeld, ertoe strekt het opschrift van de wet als volgt te wijzigen: "wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst".[5]

Gelet op de erg recente wijzigingen die in de wet van 11 december 1998 zijn aangebracht, moet de steller bijgevolg nagaan of de verwijzingen in het voorontwerp naar die wet nog correct zijn.

IV. Correcte omzetting van de CER-richtlijn

Zoals artikel 2 aangeeft, strekt het voorontwerp tot omzetting van de CER-richtlijn.

Die omzetting is onvolledig en soms niet erg transparant. Zonder exhaustief te willen zijn en zonder te vooruit te lopen op wat in de bijzondere opmerkingen zal worden uiteengezet, moet in dat verband op de volgende elementen worden gewezen:

a) Artikel 1, lid 3, van de CER-richtlijn wordt niet correct omgezet bij artikel 5, § 2, van het voorontwerp. Artikel 1, lid 3, van de CER-richtlijn bepaalt immers dat wanneer in bepalingen van sectorspecifieke rechtshandelingen van de Europese Unie wordt voorgeschreven dat kritieke entiteiten maatregelen nemen om hun weerbaarheid te vergroten, en wanneer die voorschriften door de lidstaten worden erkend als ten minste gelijkwaardig aan de in de CER-richtlijn vastgestelde overeenkomende verplichtingen, de desbetreffende bepalingen van die richtlijn niet van toepassing zijn. Artikel 5,

4 Zie bijvoorbeeld de artikelen 8, § 4, 19 en 30, § 1, van het voorontwerp.

5 Over de wet van 2 juni 2024 is op 27 februari 2024 advies 75.110/2 gegeven (*Parl.St.* Kamer 2023-24, nr. 55-3938/001, 65-90).

ainsi que des dispositions législatives et règlementaires qui, à sa suite, s'en trouveraient modifiées.

L'attention de l'auteure de l'avant-projet est plus particulièrement attirée sur l'article 20 de l'avant-projet, lequel met en place une procédure particulière lorsque "survient un événement de nature à perturber de manière importante la fourniture de services essentiels". Ce faisant, l'article 20 règle ainsi non plus la prévention d'un incident mais sa gestion après qu'il soit survenu, en manière telle que la procédure en question doit être mise en regard et le cas échéant articulée avec celle qui s'applique en matière de gestion de crise.

2. Dans le même ordre d'idées, l'avant-projet renvoie à plusieurs reprises à d'autres législations, notamment à la loi du 11 décembre 1998 'relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'[4]. Or cette loi a été modifiée récemment par une loi du 2 juin 2024 'modifiant la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', dont, par exemple, l'article 2 modifie l'intitulé de la loi comme suit: "loi relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé"[5].

L'auteure de l'avant-projet vérifiera par conséquent que les renvois à la loi du 11 décembre 1998 auxquels procède l'avant-projet examiné sont corrects au regard des modifications fort récentes qui lui ont été apportées.

IV. La correcte transposition de la directive CER

Comme l'indique son article 2, l'avant-projet tend à transposer la directive CER.

Cette transposition est incomplète et se présente parfois de manière peu transparente. À cet égard, sans être exhaustif et sans empiéter sur ce qui sera exposé dans les observations particulières, il y a lieu de faire état des éléments suivants:

a) L'article 1er, paragraphe 3, de la directive CER n'est pas correctement transposé par l'article 5, § 2, de l'avant-projet. En effet, l'article 1er, paragraphe 3, de la directive CER prévoit que les dispositions pertinentes de celle-ci ne s'appliquent pas lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités critiques qu'elles adoptent des mesures pour renforcer leur résilience et lorsque ces exigences sont reconnues par les États membres comme étant au moins équivalentes aux obligations correspondantes prévues par la directive CER. Or, l'article 5, § 2, de l'avant-projet

4 Voir par exemple les articles 8, § 4, 19 et 30, § 1er, de l'avant-projet.

5 La loi du 2 juin 2024 a fait l'objet de l'avis 75.110/2 donné le 27 février 2024 (*Doc. parl.*, Chambre, 2023-2024, n° 55-3938/001, pp. 65-90).

§ 2, van het voorontwerp beperkt de mogelijke uitzonderingen echter niet tot de gevallen waarin sprake is van bepalingen van sectorspecifieke rechtshandelingen van de Europese Unie, aangezien het slaat op "specifieke wetgeving" in het algemeen, met inbegrip dus van de nationale wetgevingen, en niet enkel op wetgeving die voortvloeit uit het recht van de Europese Unie.

b) Artikel 1, lid 4, van de CER-richtlijn wordt niet omgezet bij het voorontwerp. Het bepaalt nochtans vereisten inzake evenredigheid en relevantie van de uitwisseling van informatie die op grond van Unie- of nationale regelgeving vertrouwelijk is, in het bijzonder met betrekking tot bedrijfsinformatie, alsook de veiligheids- en commerciële belangen van kritieke entiteiten.

c) Artikel 22 van het voorontwerp voorziet niet in de omzetting van artikel 4, lid 1, tweede zin, van de CER-richtlijn, waarin wordt bepaald dat "de strategie (…), voortbouwend op bestaande nationale en sectorale strategieën, alsook op plannen of soortgelijke documenten, strategische doelstellingen en beleidsmaatregelen [bevat] die ervoor moeten zorgen dat kritieke entiteiten een hoge weerbaarheid hebben en behouden, en die ten minste op de in de bijlage beschreven sectoren betrekking hebben".

d) Zoals de gemachtigde van de minister erkend heeft, wordt de inleidende zin van artikel 6, lid 2, van de CER-richtlijn niet omgezet wat betreft de verplichting rekening te houden met de strategie van de lidstaat bij de identificatie van de kritieke entiteiten.

e) Artikel 11 van de CER-richtlijn omvat een algemene verplichting tot wederzijdse raadpleging over kritieke entiteiten, om te zorgen voor een consistente toepassing van de richtlijn. Die verplichting wordt niet omgezet bij artikel 15 van het voorontwerp, dat zich beperkt tot het voorzien van bilateraal en multilateraal overleg over bijzondere punten.

f) De gemachtigde van de minister heeft beaamd dat artikel 12, lid 2, tweede alinea, van de CER-richtlijn niet volledig wordt omgezet bij artikel 17 van het voorontwerp.

g) De gemachtigde van de minister heeft ook beaamd dat artikel 13, lid 1, tweede alinea, van de CER-richtlijn niet wordt omgezet bij artikel 18, § 3, van het voorontwerp.

h) De gemachtigde van de minister heeft beaamd dat artikel 13, lid 2, van de CER-richtlijn niet volledig wordt omgezet bij artikel 18 van het voorontwerp.

i) Luidens artikel 15, lid 1, van de CER-richtlijn is een eerste melding binnen 24 uur na de kennisname van een incident vereist, in voorkomend geval gevolgd door een gedetailleerd verslag uiterlijk een maand later. De gemachtigde van de minister beaamt dat artikel 20, § 1, van het voorontwerp dat vereiste niet overneemt. Die leemte moet aangevuld worden.

ne limite pas les exceptions possibles aux cas d'existence de dispositions d'actes juridiques sectoriels de l'Union européenne, étant donné qu'il vise, de manière générale, les "législations spécifiques", y compris donc les législations nationales et pas seulement celles qui résultent du droit de l'Union européenne.

b) L'article 1er, paragraphe 4, de la directive CER n'est pas transposé par l'avant-projet. Il fixe pourtant des exigences de proportionnalité et de nécessité relatives à l'échange d'informations qui sont confidentielles en application de règles de l'Union européenne ou du droit national, en particulier en ce qui concerne le secret des affaires, ainsi que la sécurité et les intérêts commerciaux des entités critiques.

c) L'article 4, paragraphe 1, deuxième phrase, de la directive CER, qui énonce que "[l]a stratégie définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe", n'est pas transposé par l'article 22 de l'avant-projet.

d) La phrase liminaire de l'article 6, paragraphe 2, de la directive CER n'est, comme l'a reconnu le délégué de la Ministre, pas transposée quant à l'obligation de tenir compte de la stratégie de l'État dans la recension des entités critiques.

e) L'article 11 de la directive CER comprend une obligation générale de consultation mutuelle au sujet des entités critiques aux fins d'assurer son application cohérente qui n'est pas transposée par l'article 15 de l'avant-projet, lequel se borne à prévoir des discussions multilatérales et bilatérales sur des points particuliers.

f) L'article 12, paragraphe 2, alinéa 2, de la directive CER n'a, comme en a convenu le délégué de la Ministre, pas été transposé complètement par l'article 17 de l'avant-projet.

g) Comme en a convenu également le délégué de la Ministre, l'article 13, paragraphe 1, alinéa 2, de la directive CER n'est pas transposé par l'article 18, § 3, de l'avant-projet.

h) L'article 13, paragraphe 2, de la directive CER n'a, comme en a convenu le délégué de la Ministre, pas été transposé complètement par l'article 18 de l'avant-projet.

i) L'article 15, paragraphe 1, de la directive CER comprend une exigence de première notification au plus tard 24 heures après avoir pris connaissance d'un incident, suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après; comme en a convenu le délégué de la Ministre, l'article 20, § 1er, de l'avant-projet ne reprend pas cette exigence. Cette lacune sera comblée.

j) Artikel 15, lid 3, van de CER-richtlijn wordt niet volledig omgezet bij het voorontwerp, althans wat de bescherming van de commerciële belangen en dus van het zakengeheim betreft.

k) De gemachtigde van de minister heeft beaamd dat artikel 15, lid 4, van de CER-richtlijn niet wordt omgezet bij het voorontwerp.

l) Artikel 17, lid 4, van de CER-richtlijn wordt niet omgezet bij artikel 14 van het voorontwerp.

m) Artikel 18, lid 4, vierde alinea 4, en lid 7, van de CER-richtlijn, gewijd aan de adviesmissies, wordt niet omgezet bij het voorontwerp met als reden dat het gaat om een bepaling met betrekking tot de organisatie van adviesmissies door de Europese Commissie. Dat is inderdaad het doel van artikel 18 van de CER-richtlijn, maar dat artikel bevat ook verschillende verplichtingen voor de lidstaten, met name in lid 4, vierde alinea, en in lid 7, die in het voorontwerp moeten worden opgenomen.

n) Artikel 21, lid 3, van de CER-richtlijn wordt niet correct omgezet bij artikel 33 van het voorontwerp aangezien laatstgenoemd artikel zich ertoe beperkt een ingebrekestelling van de kritieke entiteit door de inspectiedienst te voorzien.

2. Aan de hand van de concordantietabellen moet men kunnen beoordelen in welke mate de CER-richtlijn correct wordt omgezet door het voorontwerp. Die tabellen bevatten evenwel verschillende fouten en zijn soms slecht op elkaar afgestemd.

Zonder volledigheid na te streven, kunnen de volgende punten worden aangehaald:

a) In de concordantietabellen wordt melding gemaakt van een onbestaande paragraaf 4 in artikel 20 van het voorontwerp.

b) De tabel die de overeenkomst tussen de CER-richtlijn en het voorontwerp weergeeft, geeft aan dat artikel 10, lid 3, van de CER-richtlijn wordt omgezet bij artikel 21, § 3, van het voorontwerp, terwijl de tabel die de overeenkomst tussen het voorontwerp en de CER-richtlijn weergeeft, vermeldt dat artikel 10, lid 3, van de CER-richtlijn wordt omgezet bij de artikelen 27 en 28, § 1, van het voorontwerp.

c) In de tabel die de overeenkomst tussen de CER-richtlijn en het voorontwerp weergeeft, wordt vermeld dat artikel 9, lid 6, van de richtlijn wordt omgezet bij artikel 20, § 3, van het voorontwerp, terwijl het wordt omgezet bij artikel 23.

Om het Parlement correcte informatie te kunnen bezorgen, moeten die omzettingstabellen aandachtig worden nagelezen, en moeten ze ook verwijzen naar de regelgevende teksten die zijn vastgesteld of nog moeten worden vastgesteld om de CER-richtlijn in zijn geheel om te zetten.[6]

[6] Dat is met name het geval met de omzetting van artikel 13 van de CER-richtlijn, waarvoor, zoals de gemachtigde van de minister heeft beaamd, een koninklijk besluit moet worden uitgevaardigd.

j) L'article 15, paragraphe 3, de la directive CER n'est pas transposé complètement par l'avant-projet, à tout le moins en ce qui concerne la préservation des intérêts commerciaux et donc des secrets d'affaires.

k) L'article 15, paragraphe 4, de la directive CER n'est pas transposé dans l'avant-projet, comme l'a reconnu le délégué de la Ministre.

l) L'article 17, paragraphe 4, de la directive CER n'est pas transposé par l'article 14 de l'avant-projet.

m) L'article 18, paragraphes 4, alinéa 4, et 7, de la directive CER, consacrés aux missions de conseil, n'est pas transposé par l'avant-projet au motif qu'il s'agit d'une disposition concernant l'organisation de missions consultatives par la Commission européenne. Si tel est en effet l'objet de l'article 18 de la directive CER, ce dernier contient également plusieurs obligations pour les États membres, notamment au paragraphe 4, alinéa 4, et au paragraphe 7, qu'il convient de faire figurer dans l'avant-projet.

n) L'article 21, paragraphe 3, de la directive CER n'est pas correctement transposé par l'article 33 de l'avant-projet en ce que ce dernier se limite à prévoir une mise en demeure de l'entité critique par le service d'inspection.

2. Les tableaux de correspondance doivent permettre d'appréhender la mesure dans laquelle la directive CER est correctement transposée par l'avant-projet. Or, ceux-ci contiennent plusieurs erreurs et manquent parfois de coordination.

Sans prétendre à l'exhaustivité, les points suivants peuvent être relevés:

a) Les tableaux de correspondance mentionnent un paragraphe 4, inexistant, à l'article 20 de l'avant-projet.

b) Le tableau de correspondance entre la directive CER et l'avant-projet indique que l'article 10, paragraphe 3, de la directive CER est transposé par l'article 21, § 3, de l'avant-projet tandis que le tableau de correspondance entre l'avant-projet et la directive CER fait état de ce que l'article 10, paragraphe 3, de la directive CER est transposé par les articles 27 et 28, § 1er, de l'avant-projet.

c) Le tableau de correspondance entre la directive CER et l'avant-projet mentionne que l'article 9, paragraphe 6, de la directive est transposé par l'article 20, § 3, de l'avant-projet alors qu'il est transposé par son article 23.

Afin d'informer parfaitement le Parlement, ces tableaux de transposition seront attentivement relus et feront également référence aux actes réglementaires qui ont été adoptés ou doivent encore être adoptés afin de transposer la directive CER dans sa totalité[6].

[6] Tel est notamment le cas pour la transposition de l'article 13 de la directive CER pour laquelle, comme en a convenu le délégué de la Ministre, un arrêté royal doit être adopté.

Bijzondere opmerkingen

Indieningsbesluit

Het voorontwerp moet voorzien worden van een koninklijk besluit tot indiening van een wetsontwerp met het oog op indiening bij de Kamer van volksvertegenwoordigers.[7]

Opschrift

In de Franse tekst moet het woord “concernant” worden vervangen door de woorden “relative à”.

Dispositief

Artikel 1

Het voorontwerp regelt geen aangelegenheid als bedoeld in artikel 78 van de Grondwet, maar een aangelegenheid als bedoeld in artikel 74 ervan.

Artikel 1 moet in die zin worden aangepast.

Artikelen 3, 11°, en 44 en bijlage

Een overheidsinstantie wordt in artikel 3, 11°, van het voorontwerp als volgt gedefinieerd:

“een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

1° zij hangt af van de Federale Staat;

2° zij is niet van industriële of commerciële aard;

3° zij oefent niet hoofdzakelijk een activiteit uit die tot een van de andere sectoren of deelsectoren uit de bijlage behoren;

4° zij is geen privaatrechtelijke rechtspersoon.”

Artikel 44 van het voorontwerp, dat vervat is in hoofdstuk 8 met als opschrift “Sector overheid”, voorziet in een bijzondere regeling die van toepassing is op de overheidsbesturen, die overigens ressorteren onder een bijzondere sector van de bijlage, *in casu* sector 9.

Zo wordt de koning ertoe gemachtigd voor de sector overheid te bepalen, op voorstel van de sectoraal bevoegde minister, hoe de verplichtingen moeten worden uitgevoerd die voortvloeien uit de bepalingen bedoeld in artikel 44 van het voorontwerp.

Zodoende strekken die bepalingen en de bijlage tot omzetting van artikel 2, 10°, van de CER-richtlijn en van punt 9 van de bijlage van de richtlijn.

[7] *Beginselen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbeveling 226.

Observations particulières

Arrêté de présentation

L’avant-projet sera pourvu d’un arrêté royal de présentation d’un projet de loi en vue de son dépôt à la Chambre des représentants[7].

Intitulé

Dans la version française, il y a lieu de remplacer le mot “concernant” par les mots “relative à”.

Dispositif

Article 1er

L’avant-projet ne règle pas une matière visée à l’article 78 de la Constitution mais une matière visée à l’article 74 de celle-ci.

L’article 1er sera adapté en ce sens.

Articles 3, 11°, 44 et annexe

L’entité d’administration publique est définie comme suit par l’article 3, 11°, de l’avant-projet:

“une autorité administrative visée à l’article 14, § 1er, alinéa 1er, des lois coordonnées sur [le] Conseil d’État qui satisfait aux critères suivants:

1° elle dépend de l’État fédéral;

2° elle n’a pas de caractère industriel ou commercial;

3° elle n’exerce pas à titre principal une activité relevant de l’un des autres secteurs ou sous-secteurs de l’annexe:

4° elle n’est pas une personne morale de droit privé”.

L’article 44 de l’avant-projet qui figure sous le chapitre 8 de celui-ci, intitulé “Secteur des administrations publiques”, prévoit un régime particulier applicable aux administrations publiques, lesquelles relèvent d’ailleurs d’un secteur particulier de l’annexe, en l’occurrence le secteur 9.

Ainsi le Roi est-il habilité à déterminer pour le secteur des administrations publiques, sur proposition du ministre sectoriel compétent, les modalités d’exécution des obligations découlant des dispositions de l’avant-projet visées à l’article 44.

Ce faisant, ces dispositions ainsi que l’annexe tendent à transposer l’article 2, 10°, de la directive CER et le point 9 de son annexe.

[7] *Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet technique législative, recommandation n° 226.

Uit wat voorafgaat, blijkt dat de betrokken overheden worden opgevat als kritieke entiteiten die ressorteren onder een specifieke sector, waarvoor speciaal sectorale overheden moeten worden aangewezen.

In die zin stelt de bespreking van artikel 44 het volgende:

"Het wetgevend kader betreffende de kritieke entiteiten, dat historisch gezien werd opgesteld voor, en enkel werd toegepast op, de privésector, is niet zo eenvoudig op volledig dezelfde manier toepasbaar op de sector overheid. De weerbaarheid van de overheidsinstellingen in België is uiteraard minstens even belangrijk als in de privésector, doch noodzaakt de specificiteit van deze sector eigenlijk een gespecialiseerd of aangepast kader.

In de eerste plaats bemoeilijkt dit de keuze voor een sectorale overheid aangezien de scheidingslijn met de kritieke entiteit in deze sector vervaagt. Het zou daarnaast ook niet werkbaar zijn om de ene overheidsdienst aan de andere normen en verplichtingen te laten opleggen en doen afdwingen, waardoor het onmogelijk is om een algemene sectorale overheid voor de gehele sector aan te duiden. Ten slotte is de situatie voor elke federale overheidsdienst verschillend, zodat het noodzakelijk is dat elke minister zelf de invulling van de verplichtingen uit de wet kan vastleggen. Het wordt daarom niet opportuun geacht om alles in de wet zelf vast te leggen. Bijgevolg zal delegatie aan de Koning gegeven worden zodat dit sectoraal, en meer bepaald, per bevoegde minister, geregeld kan worden.

Omwille van de bovenstaande bijzondere eigenschappen van de sector overheid en de uitdagingen die deze met zich meebrengen wordt voor deze sector een bijzonder kader opgericht, gebaseerd op de verplichtingen uit de CER-Richtlijn en aangepast aan de specificiteiten van de sector. Voor deze sector zal volledig de *ratio legis* van de CER-Richtlijn gevolgd worden.

Op deze manier voldoet België aan zijn verplichting om de CER-Richtlijn tijdig om te zetten in nationale regelgeving, rekening houdend met de verschillen die bestaan tussen de private en publieke sector."

Indien, zoals uit die bespreking blijkt, de steller van het voorontwerp op die manier de verplichting tot omzetting van de CER-richtlijn wil nakomen, rekening houdend met de bestaande verschillen tussen de private en de overheidssector, dient te worden opgemerkt dat de definitie in artikel 3, 11°, van het voorontwerp tot gevolg heeft dat de richtlijn slechts gedeeltelijk wordt omgezet, voor zover de bedoelde overheidsinstanties enkel die zijn welke ressorteren onder de federale overheid.

Gelet op de beginselen betreffende de bevoegdheidsverdeling ter zake, zoals in herinnering gebracht in algemene opmerking nr. II, is het met betrekking tot de overheidsinstanties die onder de bevoegdheid van de deelstaten ressorteren inderdaad onaanvaardbaar dat de federale wetgever de gewesten eenzijdig – bij wege van een gewone wet – tot samenwerking zou dwingen (via een procedure zoals voorzien in artikel 44

Il ressort de ce qui précède que les administrations publiques concernées sont conçues comme des entités critiques qui relèvent d'un secteur particulier, pour lequel des autorités sectorielles doivent spécialement être désignées.

C'est en ce sens que le commentaire de l'article 44 précise ce qui suit:

"Le cadre législatif sur les entités critiques, historiquement rédigé et appliqué uniquement au secteur privé, n'est pas si facilement applicable de la même manière au secteur public. La résilience des institutions publiques en Belgique est évidemment au moins aussi importante que dans le secteur privé, mais la spécificité de ce secteur nécessite en fait un cadre spécialisé ou adapté.

En premier lieu, ceci complique le choix d'une autorité sectorielle, car la ligne de démarcation avec l'entité critique dans ce secteur est floue. En outre, il ne serait pas envisageable qu'une administration impose et fasse respecter des normes et des obligations a une autre, ce qui rendrait impossible la désignation d'une autorité sectorielle générale pour l'ensemble du secteur. Enfin, la situation étant différente pour chaque ministre fédéral, il est nécessaire que chaque ministre puisse définir l'interprétation des obligations prévues par la loi. Il n'est donc pas jugé opportun de tout fixer dans la loi elle-même. C'est la raison pour laquelle délégation sera donnée au Roi afin que ceci puisse être réglé sectoriellement, et plus précisément, par ministre compétent.

En raison des caractéristiques particulières du secteur public et des défis qu'il pose, un cadre spécial sera établi pour ce secteur, basé sur les obligations de la Directive CER et adapté à ses spécificités. La *ratio legis* de la Directive CER sera intégralement respectée pour ce secteur.

De cette manière, la Belgique remplit son obligation de transposer la Directive CER dans la réglementation nationale en temps voulu, en tenant compte des différences qui existent entre le secteur privé et le secteur public".

Si tel que cela ressort de ce commentaire, l'auteure de l'avant-projet entend ainsi respecter son obligation de transposer la directive CER, en tenant compte des différences qui existent entre le secteur privé et le secteur public, il y a lieu de relever que la définition que donne l'article 3, 11°, de l'avant-projet a pour effet de ne transposer que partiellement la directive dans la mesure où les administrations publiques visées sont limitées aux administrations dépendant de l'autorité fédérale.

Certes, compte tenu des principes relatifs à la répartition des compétences en la matière, tels qu'ils ont été rappelés dans l'observation générale n° II, il ne pourrait être admis, s'agissant des administrations publiques relevant des entités fédérées, que le législateur fédéral impose unilatéralement – par une loi ordinaire – une collaboration forcée des Régions (via une procédure, telle que celle prévue à l'article 44 de

van het voorontwerp, volgens welke de ministers van de deelstaten voorstellen zouden moeten doen). Om te zorgen voor de volledige omzetting van de richtlijn met betrekking tot de sector van de overheidsinstanties die niet onder de federale overheid ressorteren, zou men bij ontstentenis van een samenwerkingsakkoord dat met de betrokken deelstaten is gesloten, toepassing kunnen maken van artikel 92*ter* van de bijzondere wet van 8 augustus 1980. Dat is trouwens wat artikel 21, § 4, van het voorontwerp voorziet wanneer het stelt dat de Koning sectorale overheden kan oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de gemeenschappen en de gewesten, overeenkomstig de nadere regels bepaald in artikel 92*ter*.

Het dispositief moet in het licht van deze opmerking herzien worden. Indien niet, moet in de bespreking van het artikel worden uitgelegd hoe de omzetting van de richtlijn voor de overheidsinstanties die niet onder de federale autoriteit ressorteren, overwogen wordt in het kader van de residuaire bevoegdheid van de federale overheid inzake preventieve bescherming op het gebied van de openbare veiligheid.

Artikel 3

1. Het verdient aanbeveling in punt 1° te verwijzen naar het precieze artikel waarbij het Coördinatieorgaan voor de dreigingsanalyse wordt opgericht, te weten artikel 5 van de wet van 10 juli 2006 ‘betreffende de analyse van de dreiging’.

2. In de Franse tekst van punt 2° dient men te schrijven “par arrêté délibéré en Conseil des Ministres” in plaats van “par arrêté pris après avis du Conseil des ministres”.

Dezelfde opmerking geldt voor heel het voorontwerp.[8]

3. De definities van “kritieke entiteiten” en “entité critique” in respectievelijk de Nederlandse en de Franse tekst van punt 3° komen niet overeen. Ze moeten in overeenstemming worden gebracht.

4. De definitie in de Nederlandse tekst van punt 4° stemt niet helemaal overeen met de definitie in de CER-richtlijn. Die laatste definitie moet exact worden overgenomen zodat geen enkele twijfel bestaat over de correcte omzetting.

5. Het verdient aanbeveling in punt 10° te verwijzen naar het precieze artikel van de wet van 7 december 1998 ‘tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus’, te weten artikel 93, § 2, eerste lid, 3°.

6. In punt 12° dient de datum van de wet te worden toegevoegd, te weten 26 april 2024.

Artikel 6

Volgens paragraaf 1, 5°, zijn “de rechterlijke overheden, begrepen als de organen van de rechtelijke macht, met inbegrip

[8] Zie met name artikel 21, § 4, en de bijlage.

l’avant-projet, dans laquelle des ministres des entités fédérées seraient tenus de faire des propositions). Toutefois, pour assurer la complète transposition de la directive en ce qui concerne le secteur des administrations publiques qui ne relèvent pas de l’autorité fédérale, il pourrait, à défaut d’un accord de coopération conclu avec les entités concernées, être recouru à l’application de l’article 92*ter* de la loi spéciale du 8 août 1980. C’est du reste ce que prévoit l’article 21, § 4, de l’avant-projet lorsqu’il dispose que le Roi peut instituer des autorités sectorielles composées de représentants de l’État fédéral, des Communautés et des Régions, selon les modalités prévues à cet article 92*ter*.

Le dispositif sera revu à la lumière de l’observation. À défaut, le commentaire de l’article expliquera comment la transposition de la directive pour les administrations publiques qui ne relèvent pas de l’Autorité fédérale est envisagée dans le cadre de la compétence résiduelle de l’autorité fédérale en matière de protection préventive dans le domaine de la sécurité publique.

Article 3

1. Le 1° gagnerait à renvoyer à l’article précis instituant l’Organe de coordination pour l’analyse de la menace, à savoir l’article 5 de la loi du 10 juillet 2006 ‘relative à l’analyse de la menace’.

2. Au 2°, il convient d’écrire “par arrêté délibéré en Conseil des ministres” au lieu de “par arrêté pris après avis du Conseil des Ministres”.

La même observation vaut pour l’ensemble de l’avant-projet[8].

3. Au 3°, les définitions française et néerlandaise d’“entité critique” et de “kritieke entiteiten” ne correspondent pas. Elles devront être mises en concordance.

4. Au 4°, la version néerlandaise de la définition ne correspond pas totalement à la définition de la directive CER. Il y a lieu de reproduire celle-ci afin d’éviter tout doute quant à sa correcte transposition.

5. Le 10° gagnerait à renvoyer à l’article précis de la loi du 7 décembre 1998 ‘organisant un service de police intégré, structuré à deux niveaux’, à savoir l’article 93, § 2, alinéa 1er, 3°.

6. Au 12°, il convient d’ajouter la date de la loi, à savoir le 26 avril 2024.

Article 6

Le paragraphe 1er, 5°, exclut du champ d’application de l’avant-projet “les autorités judiciaires, entendues comme les

[8] Voir notamment l’article 21, § 4, et l’annexe.

van het Openbaar Ministerie", uitgesloten uit het toepassingsgebied van het voorontwerp, en omvatten ze niet het Grondwettelijk Hof en de Raad van State.

De steller van het voorontwerp moet nagaan of dat wel de bedoeling is, en moet in voorkomend geval die uitsluiting verantwoorden.

Artikel 7

Zoals de gemachtigde van de Minister heeft voorgesteld, moet artikel 7 worden gewijzigd zodat het uitdrukkelijk verwijst naar gedelegeerde verordening (EU) 2023/2450 van de Commissie van 25 juli 2023 'tot aanvulling van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad door de vaststelling van een lijst van essentiële diensten'.[9] Overeenkomstig artikel 5, lid 1, van de CER-richtlijn is het aan de hand van die gedelegeerde verordening dat de bevoegde autoriteiten een risicobeoordeling moeten uitvoeren.

Artikel 8

Het is niet duidelijk waarop de woorden "die vallen onder de bevoegdheid van de ondersteunende diensten" in paragraaf 2, tweede lid, betrekking hebben.

Artikel 9

1. De nummering waarmee de leden van paragraaf 1 worden aangeduid, is overbodig. Ze moet worden weggelaten.

2. Aangezien de "NIS 2-wet" wordt gedefinieerd in artikel 3, 12°, van het voorontwerp, hoeft in paragraaf 4 niet het volledige opschrift te worden herhaald. Het voorontwerp moet op dat punt worden gewijzigd.

Artikel 11

Er wordt bepaald dat de "sectorale overheid (…) sectorale criteria [kan] bepalen waaraan de kritieke entiteiten moeten voldoen, rekening houdend met de bijzondere eigenschappen van de betrokken sector".

Zodoende verleent de voorliggende bepaling een verordenende bevoegdheid aan de sectorale overheden.

Uit de bijlage blijkt evenwel dat de sectorale overheid niet per se een minister is.

Met betrekking tot het toekennen van een verordenende bevoegdheid aan een overheid die geen politieke verantwoording hoeft af te leggen bij de betrokken wetgevende vergaderingen – dat wil zeggen aan een andere overheid dan de regering of een Minister –, heeft de afdeling Wetgeving

[9] *https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202302450.*

organes du pouvoir judiciaire, le Ministère public inclus" sans que cela n'englobe la Cour constitutionnelle et le Conseil d'État.

L'auteure de l'avant-projet vérifiera si cela correspond bien à son intention et justifiera, le cas échéant, cette exclusion.

Article 7

Comme suggéré par le délégué de la Ministre, l'article 7 sera modifié pour renvoyer expressément au règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 'complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels'[9]. Conformément à l'article 5, paragraphe 1, de la directive CER, ce règlement délégué doit être utilisé par les autorités compétentes pour effectuer une évaluation des risques.

Article 8

Au paragraphe 2, alinéa 2, il n'apparaît pas clairement à quoi se rapportent les mots ", qui relèvent de la compétence des services d'appui,".

Article 9

1. Le paragraphe 1er contient une numérotation superflue pour désigner les alinéas. Elle sera supprimée.

2. Étant donné que la "loi NIS 2" est définie à l'article 3, 12°, de l'avant-projet, il n'est pas nécessaire de répéter son intitulé complet au paragraphe 4. L'avant-projet sera modifié sur ce point.

Article 11

Il est prévu que "[l]'autorité sectorielle peut déterminer des critères sectoriels auxquels doivent répondre les entités critiques en tenant compte des particularités du secteur concerné".

Ce faisant, la disposition examinée confère un pouvoir réglementaire aux autorités sectorielles.

Or, il ressort de l'annexe que l'autorité sectorielle n'est pas forcément un ministre.

Concernant l'attribution d'un pouvoir réglementaire à une autorité qui n'est pas responsable politiquement devant les assemblées législatives concernées – c'est-à-dire, à une autorité autre que le gouvernement ou qu'un Ministre –, la section de législation a déjà observé à de nombreuses

[9] *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202302450.*

in het verleden al meermaals opgemerkt dat het toekennen van een verordeningsbevoegdheid aan overheidsinstanties of hun organen moeilijk verenigbaar is met de algemene beginselen van het Belgische publiekrecht (artikelen 33 en 108 van de Grondwet), aangezien het raakt aan het beginsel van de eenheid van de verordenende macht en aangezien ter zake iedere rechtstreekse parlementaire controle ontbreekt. Verordeningen van die aard ontberen daarenboven de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking en de preventieve controle van de afdeling Wetgeving.

In het verleden heeft de afdeling Wetgeving weliswaar reeds bepaalde uitzonderingen op het verbod van delegatie van een verordenende bevoegdheid aan openbare instellingen aanvaardbaar geacht, maar dan ging het doorgaans om delegaties met een beperkte draagwijdte en van een zodanig technische aard dat men ervan kon uitgaan dat de instanties die de betrokken regelgeving moesten toepassen, ook het best geplaatst waren om ze uit te werken.[10]

Zelfs in die gevallen heeft de afdeling Wetgeving reeds opgemerkt dat het niettemin belangrijk is dat die verordeningen tot stand komen via een beslissing van de uitvoerende macht op voorstel van de instantie, of op zijn minst door de uitvoerende macht worden goedgekeurd, en dat ze zodoende worden bekendgemaakt in het *Belgisch Staatsblad*.[11] Op die manier wordt de verantwoordelijkheid voor de betrokken verordening opgenomen door een overheid die aan de wetgevende kamers politieke verantwoording verschuldigd is.

Artikel 11 moet in het licht van deze opmerking worden herzien.

Artikel 12

1. In de bespreking van paragraaf 1, tweede lid, staat dat de “gefedereerde entiteiten (…) eveneens [zullen] kunnen worden geraadpleegd door de sectorale overheden vóór de aanduiding voor wat de kritieke entiteiten betreft van sectoren die onder hun bevoegdheden vallen”, terwijl in het dispositief wordt bepaald dat de dossiers “ter informatie” naar de deelstaten worden gezonden.

Op een vraag in dat verband heeft de gemachtigde van de Minister het volgende geantwoord:

“De raadpleging waarnaar verwezen wordt in dit artikel betreft eigenlijk de raadpleging die doorheen de gehele

[10] Zie bijvoorbeeld advies 42.387/VR van 27 maart 2007 over een voorontwerp dat heeft geleid tot de wet van 15 mei 2007 ‘houdende instemming met het samenwerkingsakkoord tussen de Federale Overheid, het Vlaamse Gewest, het Waalse Gewest en het Brussels Hoofdstedelijk Gewest inzake de uitvoering van sommige bepalingen van het Protocol van Kyoto, afgesloten te Brussel, op 19 februari 2007’ (*Parl.St.* Senaat 2006-07, nr. 51-2411/001, 30-35) en advies 63.288/4 van 30 april 2018 over een voorontwerp dat heeft geleid tot de wet van 19 juli 2018 ‘inzake toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties’ (*Parl.St.* Kamer 2017-18, nr. 54-3159/001, 25-29).

[11] Zie advies 63.288/4.

reprises que l’attribution d’une compétence réglementaire à des organismes publics ou à leurs organes est difficilement compatible avec les principes généraux du droit public belge (article 33 et 108 de la Constitution) en ce qu’elle porte atteinte au principe de l’unité du pouvoir réglementaire et échappe à tout contrôle parlementaire direct. Les actes réglementaires de ce type sont en outre dépourvus des garanties dont est assortie la réglementation classique, telles celles en matière de publication et de contrôle préventif exercé par la section de législation.

Si, dans le passé, celle-ci a déjà estimé admissibles certaines exceptions à l’interdiction de déléguer une compétence réglementaire à des organismes publics, il s’agissait généralement de délégations de portée limitée et d’une technicité telle qu’il pouvait être considéré que les organismes qui devaient appliquer la réglementation concernée étaient également les mieux placés pour l’élaborer[10].

Même dans ces hypothèses, la section de législation a déjà observé qu’il importe cependant que ces règlements fassent l’objet d’une décision prise par le pouvoir exécutif sur proposition de l’organisme, ou à tout le moins d’une approbation par le pouvoir exécutif et, ce faisant, d’une publication au *Moniteur belge*[11]. De tels mécanismes permettent que la responsabilité du règlement concerné soit endossée par une autorité qui est responsable politiquement devant les chambres législatives.

L’article 11 sera revu à la lumière de cette observation.

Article 12

1. Le commentaire du paragraphe 1er, alinéa 2, indique que “[l]es entités fédérées pourront également être consultées par les autorités sectorielles avant la désignation pour ce qui concerne les entités critiques de secteurs qui relèvent de leurs compétences” tandis que le dispositif prévoit d’envoyer le dossier aux entités fédérées “pour information”.

Interrogé sur ce point, le délégué de la Ministre a indiqué ce qui suit:

“De raadpleging waarnaar verwezen wordt in dit artikel betreft eigenlijk de raadpleging die doorheen de gehele

[10] Voir, par exemple, l’avis 42.387/VR donné le 27 mars 2007 sur un avant-projet devenu la loi du 15 mai 2007 ‘portant assentiment à l’accord de coopération entre l’Autorité fédérale, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à la mise en œuvre de certaines dispositions du Protocole de Kyoto’, conclu à Bruxelles, le 19 février 2007 (*Doc. parl.*, Sénat, 2006-2007, n° 51-2411/001, pp. 30-35) et l’avis 63.288/4 donné le 30 avril 2018 sur un avant-projet devenu la loi du 19 juillet 2018 ‘relative à l’accessibilité des sites internet et des applications mobiles des organismes du secteur public’ (*Doc. parl.*, Chambre, 2017-2018, n° 54-3159/001, pp. 25-29).

[11] Voir l’avis 63.288/4.

identificatieprocedure heeft plaatsgevonden. Op het moment dat het dossier werd afgewerkt, is het enkel de bedoeling om het dossier, in voorkomend geval, ter informatie over te maken aan de gefedereerde entiteiten.

We stellen voor om de memorie van toelichting te aligneren met het dispositief."

De bespreking moet dienovereenkomstig worden aangepast.

2. Aan de gemachtigde van de minister is gevraagd of artikel 12, § 3, van het voorontwerp zorgt voor een correcte omzetting van artikel 6, lid 5, van de CER-richtlijn, aangezien het de voorwaarde dat de lijst van kritieke entiteiten indien nodig wordt geëvalueerd en geactualiseerd, niet overneemt, evenmin als de voorwaarde dat kennis wordt gegeven van het feit dat een entiteit niet langer als kritiek wordt beschouwd en niet meer aan de verplichtingen is onderworpen. De gemachtigde van de minister heeft het volgende geantwoord:

"Het voorontwerp gaat voor wat betreft de passage uit artikel 6, paragraaf 5, met betrekking tot de evaluatie en actualisering van de lijst van kritieke entiteiten, zelfs verder dan wat opgelegd wordt door de CER Richtlijn door te verplichten dat de sectorale overheid ten minste elke vier jaar het identificatieproces zoals omschreven in de wet opnieuw moet uitvoeren, en dus niet louter moeten evalueren. Bijgevolg wordt de lijst ten minste bij de heruitvoering van het identificatieproces volledig geactualiseerd.

Gelet op de *ratio legis* van de wetgeving rond kritieke entiteiten zoals die vandaag de dag ook bestaat en het belang van de bescherming van kritieke entiteiten die essentiële diensten verlenen in België, werd de laatste zin met betrekking tot kritieke entiteiten die niet meer worden aanzien als kritieke entiteiten ingevolge de herziening van de identificatieprocedure, niet hernomen aangezien deze identificatie en aanduiding gebeurt op basis van objectieve criteria en kritieke entiteiten worden geacht hieraan te blijven voldoen, tenzij bij volledige stopzetting van haar activiteiten of in het geval van substantiële wijzigingen in de activiteiten van de kritieke entiteit waardoor men niet meer zou voldoen aan de criteria.

Ter volledigheid van de omzetting kan in die zin aan artikel 12, § 3, van het voorontwerp een lid worden toegevoegd waarin wordt gespecifieerd dat wanneer na de uitvoering van het identificatieproces blijkt dat een eerder aangeduide kritieke entiteit niet meer voldoet aan de criteria uit artikel 10, en bijgevolg niet meer als kritieke entiteit kan worden aangeduid, de bevoegde sectorale overheid deze kritieke entiteit tijdig in kennis stelt dat zij niet meer moeten voldoen aan de verplichtingen uit deze wet".

De afdeling Wetgeving stelt vooreerst vast dat artikel 12, § 3, van het voorontwerp, in tegenstelling tot artikel 6, lid 5, van de CER-richtlijn, niet voorziet in een evaluatie, noch, in voorkomend geval, in een actualisering van de lijst van de kritieke entiteiten "wanneer dat nodig is". Het voorontwerp moet op dat punt worden aangevuld.

identificatieprocedure heeft plaatsgevonden. Op het moment dat het dossier werd afgewerkt, is het enkel de bedoeling om het dossier, in voorkomend geval, ter informatie over te maken aan de gefedereerde entiteiten.

We stellen voor om de memorie van toelichting te aligneren met het dispositief".

Le commentaire sera modifié en conséquence.

2. Interrogé sur la question de savoir si l'article 12, § 3, de l'avant-projet transpose correctement l'article 6, paragraphe 5, de la directive CER et ce que la condition de réexamen et de mise à jour de la liste des entités critiques lorsque c'est nécessaire n'est pas reproduite ainsi que la notification du fait de ne plus être recensé en tant qu'entité critique et de ne plus être soumis aux obligations n'est pas reprise, le délégué de la Ministre a indiqué ce qui suit:

"Het voorontwerp gaat voor wat betreft de passage uit artikel 6, paragraaf 5, met betrekking tot de evaluatie en actualisering van de lijst van kritieke entiteiten, zelfs verder dan wat opgelegd wordt door de CER Richtlijn door te verplichten dat de sectorale overheid ten minste elke vier jaar het identificatieproces zoals omschreven in de wet opnieuw moet uitvoeren, en dus niet louter moeten evalueren. Bijgevolg wordt de lijst ten minste bij de heruitvoering van het identificatieproces volledig geactualiseerd.

Gelet op de *ratio legis* van de wetgeving rond kritieke entiteiten zoals die vandaag de dag ook bestaat en het belang van de bescherming van kritieke entiteiten die essentiële diensten verlenen in België, werd de laatste zin met betrekking tot kritieke entiteiten die niet meer worden aanzien als kritieke entiteiten ingevolge de herziening van de identificatieprocedure, niet hernomen aangezien deze identificatie en aanduiding gebeurt op basis van objectieve criteria en kritieke entiteiten worden geacht hieraan te blijven voldoen, tenzij bij volledige stopzetting van haar activiteiten of in het geval van substantiële wijzigingen in de activiteiten van de kritieke entiteit waardoor men niet meer zou voldoen aan de criteria.

Ter volledigheid van de omzetting kan in die zin aan artikel 12, § 3, van het voorontwerp een lid worden toegevoegd waarin wordt gespecifieerd dat wanneer na de uitvoering van het identificatieproces blijkt dat een eerder aangeduide kritieke entiteit niet meer voldoet aan de criteria uit artikel 10, en bijgevolg niet meer als kritieke entiteit kan worden aangeduid, de bevoegde sectorale overheid deze kritieke entiteit tijdig in kenNIS stelt dat zij niet meer moeten voldoen aan de verplichtingen uit deze wet".

La section de législation constate tout d'abord que, contrairement à l'article 6, paragraphe 5, de la directive CER, l'article 12, § 3, de l'avant-projet ne prévoit pas un réexamen et, s'il y a lieu, une mise à jour de la liste des entités critiques "si nécessaire". L'avant-projet sera complété sur ce point.

Wat het vereiste van de kennisgeving betreft, lijken er op basis van het antwoord van de gemachtigde van de Minister twee mogelijkheden te zijn: ofwel de verplichtingen exact overnemen zoals ze in artikel 6, lid 5, van de CER-richtlijn staan, ofwel – aangezien de richtlijn strekt tot minimale harmonisatie – ervan uitgaan dat de als kritiek beschouwde entiteiten blijvend worden beschouwd als kritiek, zolang ze hun activiteiten niet volledig stopzetten of substantieel wijzigen.

Het staat aan de steller van het voorontwerp de knoop door te hakken en het dispositief alsook de bespreking van het artikel dienovereenkomstig aan te passen.

3. Op de vraag of het voorontwerp artikel 6, lid 4, van de CER-richtlijn correct omzet, met name wat betreft de verplichting te melden welke de kritieke entiteiten zijn, heeft de gemachtigde van de Minister het volgende geantwoord:

"We erkennen dat artikel 6 paragraaf 4 van de CER Richtlijn onvoldoende werd gespecifieerd in het dispositief van het voorontwerp en stellen voor om volgende paragraaf toe te voegen aan artikel 12 om hieraan tegemoet te komen:

Art. 12, § 4 'De autoriteit bedoeld in artikel 21, § 1 stelt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2 wet binnen een maand na de aanduiding bedoeld in de eerste paragraaf in kennis van de entiteiten die werden aangeduid [als] kritieke entiteiten.

Daarbij wordt, indien van toepassing, vermeld dat het entiteiten betreft die vallen onder de uitzondering van artikel 5 van deze wet'."

De afdeling Wetgeving kan zich vinden in het voorstel van de gemachtigde op voorwaarde dat nader wordt bepaald dat het gaat om de uitzondering vervat in artikel 5, § 1, van de wet.

Artikel 13

1. Paragraaf 1 behelst niet alle verplichtingen die uit artikel 6, lid 3, van de CER-richtlijn voortvloeien. Meer bepaald gaat het hier enerzijds om de verplichting dat de lidstaten de kritieke entiteiten informeren over de verplichtingen waaraan deze krachtens de hoofdstukken III en IV moeten voldoen en over de datum vanaf wanneer die verplichtingen, onverminderd artikel 8, op hen van toepassing zijn. Anderzijds gaat het om de verplichting dat de lidstaten de kritieke entiteiten van de sectoren, vermeld in de punten 3, 4 en 8 van de tabel van de bijlage, informeren dat deze geen verplichtingen hebben uit hoofde van de hoofdstukken III en IV, tenzij in nationale maatregelen anders wordt bepaald. Op een vraag over die punten heeft de gemachtigde van de Minister het volgende geantwoord:

"De met redenen omklede beslissing tot de aanduiding als kritieke entiteit bevat alle nodige gegevens met betrekking tot de verplichtingen waaraan men moet voldoen en de datum wanneer deze in werking treden. Deze kennisgeving gebeurt vandaag reeds op basis van de KI-wet, waarin het vaste praktijk

Concernant l'exigence de la notification, sur la base de la réponse du délégué de la Ministre, deux options semblent possibles: soit reprendre strictement les obligations présentes à l'article 6, paragraphe 5, de la directive CER, soit – étant donné que la directive est d'harmonisation minimale – considérer que les entités jugées critiques ne peuvent cesser de l'être sauf en cas de fin complète de leurs activités ou en cas de modifications substantielles de ces dernières.

Il revient à l'auteure de l'avant-projet de trancher et d'adapter le dispositif ainsi que le commentaire de l'article en conséquence.

3. Interrogé sur la correcte transposition de l'article 6, paragraphe 4, de la directive CER par l'avant-projet, notamment quant à l'exigence de notification de l'identité des entités critiques, le délégué de la Ministre a indiqué ce qui suit:

"We erkennen dat artikel 6 paragraaf 4 van de CER Richtlijn onvoldoende werd gespecifieerd in het dispositief van het voorontwerp en stellen voor om volgende paragraaf toe te voegen aan artikel 12 om hieraan tegemoet te komen:

Art. 12, § 4 'De autoriteit bedoeld in artikel 21, § 1 stelt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2 wet binnen een maand na de aanduiding bedoeld in de eerste paragraaf in kennis van de entiteiten die werden aangeduid [als] kritieke entiteiten.

Daarbij wordt, indien van toepassing, vermeld dat het entiteiten betreft die vallen onder de uitzondering van artikel 5 van deze wet'".

La section de législation peut se rallier à la proposition du délégué moyennant la précision qu'il s'agit de l'exception de l'article 5, § 1er, de la loi.

Article 13

1. Le paragraphe 1er ne recouvre pas l'entièreté des obligations découlant de l'article 6, paragraphe 3, de la directive CER. Il s'agit en particulier, d'une part, de l'obligation pour les États membres d'informer les entités critiques des obligations qui leur incombent en vertu des chapitres III et IV et de la date à partir de laquelle ces obligations leur sont applicables sans préjudice de l'article 8 et, d'autre part, de l'obligation d'informer les entités critiques des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres III et IV, sauf mesures nationales contraires. Interrogé sur ces points, le délégué de la Ministre a indiqué ce qui suit:

"De met redenen omklede beslissing tot de aanduiding als kritieke entiteit bevat alle nodige gegevens met betrekking tot de verplichtingen waaraan men moet voldoen en de datum wanneer deze in werking treden. Deze kennisgeving gebeurt vandaag reeds op basis van de KI-wet, waarin het vaste praktijk

is voor de sectorale overheden om alle relevante informatie hierin op te nemen.

In artikel 5 van het voorontwerp wordt gespecifieerd dat de bepalingen van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en 7 niet van toepassing zijn op de als kritiek geïdentificeerde entiteiten in de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuren.

Indien nodig, stellen we voor om te specifiëren in het dispositief dat de met redenen omklede beslissing informatie bevat over de verplichtingen waaraan de kritieke entiteit moet voldoen en vanaf wanneer deze verplichtingen nageleefd dienen te worden."

Uit de rechtspraak van het Hof van Justitie van de Europese Unie blijkt dat bepalingen van een richtlijn moeten worden uitgevoerd met een onbetwistbare dwingende kracht en met de specificiteit, nauwkeurigheid en duidelijkheid die nodig zijn om te voldoen aan het vereiste van rechtszekerheid, en dat eenvoudige administratieve praktijken, die naar hun aard volgens goeddunken van de autoriteiten kunnen worden gewijzigd en waaraan onvoldoende bekendheid is gegeven, niet als een geldige nakoming van de verplichtingen tot omzetting van een richtlijn mogen worden beschouwd.[12]

Bijgevolg dient, zoals de gemachtigde van de Minister heeft voorgesteld, in het voorontwerp uitdrukkelijk te worden vermeld dat de lidstaten verplicht zijn de kritieke entiteiten te informeren over de verplichtingen die zij hebben uit hoofde van de hoofdstukken III en IV en over de datum vanaf wanneer die verplichtingen, onverminderd de bepalingen die voor bepaalde sectoren gelden, op hen van toepassing zijn.

2. In de bespreking staat:

"Artikel 13 bepaalt de vormvoorschriften voor de aanduiding van de kritieke entiteit, namelijk de betekening van de gemotiveerde beslissing aan de kritieke entiteit met ontvangstbewijs.

Het is belangrijk dat men precies kan bepalen op welke datum de betekening van de aanduiding is gebeurd, omdat dat het startpunt is voor de termijn voor de verplichtingen van de kritieke entiteit. (…)"

Van de voorwaarde inzake het ontvangstbewijs wordt evenwel geen gewag gemaakt in het dispositief, dat op dat punt moet worden aangevuld.

3. In de bespreking staat voorts:

"Wanneer de aanduiding van een kritieke entiteit meerdere sectoren of deelsectoren aanbelangt, brengt het NCCN de bevoegde sectorale overheden samen voor overleg tussen de sectorale overheden zodat er voor de kritieke entiteiten geen dubbele verplichtingen bestaan. Tijdens het overleg kunnen bijvoorbeeld afspraken gemaakt worden met betrekking tot de inspecties en audits. (…)"

[12] Zie HJEU 30 juni 2016, nr. C-648/13, ECLI:EU:C:2016:490, *Commissie v. Polen*, § 78 en § 79.

is voor de sectorale overheden om alle relevante informatie hierin op te nemen.

In artikel 5 van het voorontwerp wordt gespecifieerd dat de bepalingen van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en 7 niet van toepassing zijn op de als kritiek geïdentificeerde entiteiten in de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuren.

Indien nodig, stellen we voor om te specifiëren in het dispositief dat de met redenen omklede beslissing informatie bevat over de verplichtingen waaraan de kritieke entiteit moet voldoen en vanaf wanneer deze verplichtingen nageleefd dienen te worden".

Il ressort de la jurisprudence de la Cour de justice de l'Union européenne que les dispositions d'une directive doivent être mises en œuvre avec une force contraignante incontestable, avec la spécificité, la précision et la clarté requises, afin que soit satisfaite l'exigence de sécurité juridique et que de simples pratiques administratives, par nature modifiables au gré de l'administration et dépourvues d'une publicité adéquate, ne sauraient être considérées comme constituant une exécution valable des obligations de transposition d'une directive[12].

Par conséquent, comme proposé par le délégué de la Ministre, il y a lieu de mentionner explicitement dans l'avant-projet l'obligation pour les États membres d'informer les entités critiques des obligations qui leur incombent en vertu des chapitres III et IV et de la date à partir de laquelle ces obligations leur sont applicables, sans préjudice des dispositions valant pour certains secteurs.

2. Le commentaire indique que

"[l]'article 13 détermine les prescriptions de forme pour la désignation de l'entité critique, à savoir la notification de la décision motivée à l'entité critique avec accusé de réception.

Il est important de pouvoir déterminer avec précision la date de la notification de la désignation, car il s'agit du point de départ du délai pour les obligations de l'entité critique […]".

La condition d'accusé de réception ne figure toutefois pas dans le dispositif. Celui-ci sera complété sur ce point.

3. Le commentaire poursuit de la sorte:

"Lorsque la désignation d'une entité critique concerne plusieurs secteurs ou sous-secteurs, le NCCN réunit les autorités sectorielles compétentes pour une consultation entre les autorités sectorielles afin d'éviter la duplication des obligations des entités critiques. Au cours de cette concertation, des accords peuvent être conclus sur les inspections et les audits, par exemple".

[12] Voir C.J.U.E., arrêt *Commission c. Pologne*, 30 juin 2016, C-648/13, ECLI:EU:C:2016:490, §§ 78-79.

Er is evenwel geen overeenstemmende paragraaf in artikel 13.

Op de vraag of het niet wenselijk is die passage op te nemen in het dispositief, heeft de gemachtigde van de Minister het volgende geantwoord:

"De paragraaf uit de Memorie van Toelichting waarnaar verwezen wordt, betreft een loutere verduidelijking van de coördinerende en faciliterende rol van het NCCN, alsook van de praktische afspraken die gemaakt kunnen worden tussen sectorale overheden. Wij zien daarom op dit moment geen meerwaarde om dit toe te voegen aan het dispositief, maar we kunnen overwegen om de verwoording te verduidelijken in de Memorie van Toelichting zodat duidelijker blijkt dat het geen verplichting, maar eerder een facultatieve uitwerking van de coördinerende opdracht van het NCCN betreft."

Zoals de gemachtigde van de Minister oppert, verdient het aanbeveling de bespreking van het artikel op dat punt aan te vullen zodat duidelijk wordt dat het niet om een verplichting gaat.

Artikel 14

Paragraaf 1 strekt tot omzetting van artikel 17, lid 1, van de CER-richtlijn. Die omzetting is evenwel onvolledig.

Ten eerste staat in paragraaf 1 dat de kritieke entiteit essentiële diensten moet verlenen "aan of in meer dan 6 lidstaten", terwijl artikel 17, lid 1, van de CER-richtlijn als voorwaarde stelt dat de kritieke entiteit dezelfde of soortgelijke essentiële diensten verleent "aan of in ten minste zes lidstaten". Het dispositief van het voorontwerp moet herzien worden zodat het beter overeenstemt met de richtlijn. Deze opmerking geldt eveneens voor paragraaf 2.

Vervolgens verwijst paragraaf 1 van de voorliggende bepaling naar artikel 13, § 1, van het voorontwerp, dus naar de kennisgeving van het feit dat de entiteit een kritieke entiteit is, terwijl artikel 17, lid 1, c), van de CER-richtlijn verwijst naar de kennisgeving van het feit dat de entiteit een kritieke entiteit van Europees belang is.

Voorts is de samenhang tussen artikel 14, § 2, tweede lid, van het voorontwerp en paragraaf 3 van hetzelfde artikel niet duidelijk. Als een en ander niet nader verduidelijkt wordt, ziet de afdeling Wetgeving immers niet in hoe het mogelijk is in paragraaf 2, tweede lid, te bepalen dat de sectorale overheid de in artikel 21, § 1, bedoelde autoriteit moet inlichten wanneer een kritieke entiteit essentiële diensten levert aan of in ten minste zes lidstaten, en vervolgens in paragraaf 3 te bepalen dat de sectorale overheid "op de hoogte gebracht [wordt] door de autoriteit bedoeld in artikel 21, § 1". Wat dat betreft, dient het dispositief van het voorontwerp te worden aangevuld zodat rekening wordt gehouden met artikel 17, lid 2 en 3, van de CER-richtlijn, waaruit voortvloeit dat de informatie die door de sectorale overheid meegedeeld wordt aan de in artikel 21, § 1, bedoelde autoriteit, vervolgens moet worden doorgegeven aan de Europese Commissie – die dan moet vaststellen of een entiteit moet worden beschouwd als een kritieke entiteit

Il n'existe toutefois pas de paragraphe correspondant dans l'article 13.

Interrogé sur l'opportunité d'inclure ce passage dans le dispositif, le délégué de la Ministre a indiqué ce qui suit:

"De paragraaf uit de Memorie van Toelichting waarnaar verwezen wordt, betreft een loutere verduidelijking van de coördinerende en faciliterende rol van het NCCN, alsook van de praktische afspraken die gemaakt kunnen worden tussen sectorale overheden. Wij zien daarom op dit moment geen meerwaarde om dit toe te voegen aan het dispositief, maar we kunnen overwegen om de verwoording te verduidelijken in de Memorie van Toelichting zodat duidelijker blijkt dat het geen verplichting, maar eerder een facultatieve uitwerking van de coördinerende opdracht van het NCCN betreft".

Comme le suggère le délégué de la Ministre, le commentaire de l'article sera utilement complété sur ce point pour clarifier qu'il ne s'agit pas d'une obligation.

Article 14

Le paragraphe 1er tend à transposer l'article 17, paragraphe 1, de la directive CER. Cette transposition est toutefois incomplète.

Tout d'abord, alors que l'article 17, paragraphe 1, de la directive CER fixe comme condition le fait que l'entité critique fournisse les mêmes services essentiels ou des services essentiels similaires "à ou dans six États membres ou plus", le paragraphe 1er indique qu'elle doit fournir des services essentiels "à ou dans plus de 6 États membres". Le dispositif de l'avant-projet sera revu afin de mieux concorder avec la directive, l'observation valant également pour le paragraphe 2.

Ensuite, alors que l'article 17, paragraphe 1, c), de la directive CER renvoie à la notification que l'entité est une entité critique d'importance européenne, le paragraphe 1er de la disposition examinée renvoie à l'article 13, § 1er, de l'avant-projet, soit la notification en tant qu'entité critique.

Par ailleurs, l'articulation entre l'article 14, § 2, alinéa 2, de l'avant-projet et le paragraphe 3 du même article n'apparaît pas clairement. En effet, sans autre précision, la section de législation n'aperçoit pas comment, alors que le paragraphe 2, alinéa 2, prévoit que c'est à l'autorité sectorielle d'informer l'autorité visée à l'article 21, § 1er, lorsqu'une entité critique fournit des services essentiels à ou dans au moins six États membres, il est possible ensuite de prévoir, au paragraphe 3, que l'autorité sectorielle est "informée par l'autorité visée à l'article 21, § 1er". Il convient à cet égard de compléter le dispositif de l'avant-projet en tenant compte de l'article 17, paragraphes 2 et 3, de la directive CER, dont il ressort que l'information communiquée par l'autorité sectorielle à l'autorité visée à l'article 21, § 1er, doit ensuite être communiquée à la Commission européenne, à qui il appartient d'établir qu'une entité doit être considérée comme une entité critique d'importance européenne et que c'est cette décision qui est ensuite

van Europees belang – en dat het die beslissing is die daarna wordt meegedeeld aan de in artikel 21, § 1, bedoelde autoriteit, die dan op haar beurt de sectorale overheid inlicht.

Tot slot heeft de gemachtigde van de Minister beaamd dat artikel 14, § 3, van het voorontwerp niet de verplichting overneemt die vervat is in artikel 17 van de CER-richtlijn, namelijk de verplichting de betrokken kritieke entiteit mee te delen welke verplichtingen voor haar gelden en vanaf welke datum. Wat dat punt betreft, heeft de gemachtigde van de Minister de volgende tekst voorgesteld, waarmee de afdeling Wetgeving akkoord kan gaan:

"Elle l'informe également des obligations supplémentaires qui lui incombent et de la date à partir de laquelle ces obligations sont applicables."

Het voorontwerp moet op die punten herzien worden zodat de richtlijn correct wordt omgezet.

Artikel 15

Het is de afdeling Wetgeving niet duidelijk hoe aan het centraal contactpunt moet worden meegedeeld dat een kritieke infrastructuur fysiek verbonden is met twee of meer lidstaten. Er moet op worden toegezien dat dit in de bespreking van het artikel extra wordt verduidelijkt.

Artikel 18

De verwijzing naar "artikel 18" in paragraaf 3, 1°, e), moet aanvullend vermelden dat het gaat om artikel 18 van de wet van 11 december 1998 'betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst'.

Artikel 20

Paragraaf 2 bevat een delegatie aan de minister van Binnenlandse Zaken om de nadere regels vast te stellen voor de kennisgeving door de Communicatie- en informatiedienst van het arrondissement (SICAD).

Op een vraag in dat verband heeft de gemachtigde van de Minister het volgende geantwoord:

"We stellen voor om de delegatie aan de Minister weg te laten aangezien het louter gaat om een bevestiging van de bestaande modaliteiten betreffende de werking van het SICAD en zo potentiële verwarring te voorkomen."

Paragraaf 2 moet in die zin gewijzigd worden.

communiquée à l'autorité visée à l'article 21, § 1er, laquelle en informe l'autorité sectorielle.

Enfin, comme en a convenu le délégué de la Ministre, l'article 14, § 3, de l'avant-projet ne reprend pas l'obligation, figurant à l'article 17 de la directive CER, d'informer l'entité critique concernée des obligations qui lui incombent et de la date à partir de laquelle ces obligations sont applicables. Sur ce point, le délégué de la Ministre a proposé le texte suivant, auquel la section de législation peut se rallier:

"Elle l'informe également des obligations supplémentaires qui lui incombent et de la date à partir de laquelle ces obligations sont applicables".

L'avant-projet sera revu sur ces points afin de transposer correctement la directive.

Article 15

La section de législation n'aperçoit pas comment le point de contact central sera informé de ce qu'une infrastructure critique est physiquement connectée avec deux États membres ou plus. Le commentaire de l'article veillera à apporter des éclaircissements supplémentaires sur ce point.

Article 18

Le renvoi effectué "à l'article 18" dans le paragraphe 3, 1°, e), sera complété pour indiquer qu'il s'agit de l'article 18 de la loi du 11 décembre 1998 'relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé'.

Article 20

Le paragraphe 2 contient une délégation au ministre de l'Intérieur pour définir les modalités de la notification par le Service d'information et de communication de l'arrondissement (SICAD).

Interrogé sur ce point, le délégué de la Ministre a indiqué ce qui suit:

"We stellen voor om de delegatie aan de Minister weg te laten aangezien het louter gaat om een bevestiging van de bestaande modaliteiten betreffende de werking van het SICAD en zo potentiële verwarring te voorkomen".

Le paragraphe 2 sera modifié en ce sens.

Artikelen 21, 27 en 28

Naar aanleiding van de vraag of artikel 10, lid 3, van de CER-richtlijn correct omgezet wordt bij de artikelen 21, § 3, 27 en 28, § 1, van het voorontwerp, heeft de gemachtigde de volgende uitleg gegeven:

"In principe zijn kritieke entiteiten gehouden aan de beperkte verspreiding en het beroepsgeheim. Volgens artikel 10 van de CER Richtlijn dient het faciliteren te gebeuren o.a. overeenkomstig het nationaal recht met betrekking tot gevoelige informatie. Daarnaast kan de Koning wel de coördinerende rol van het NCCN met betrekking tot de weerbaarheid van kritieke entiteiten verder uitwerken, inclusief het faciliteren van informatie delen tussen kritieke entiteiten, maar wel steeds rekening houdend met de behandeling van gevoelige informatie.

Onzes inziens valt het bepalen van duidelijke grenzen waarbinnen kritieke entiteiten vrijwillig informatie kunnen delen ook onder deze faciliterende taak, wat deze bepaling van het dispositief ook duidelijk beoogt.

Indien nodig, bestaat er een mogelijkheid om een verwijzing naar deze facilitatie-rol van het NCCN duidelijker op te nemen in het voorontwerp van wet, hetzij in de onderhavige bepaling ('In voorkomend geval, en wanneer zij van oordeel is dat dit opportuun is, kan de autoriteit bedoeld in art. 21, § 1, voorzien in de verdere facilitatie van het vrijwillig delen van informatie tussen kritieke entiteiten over aangelegenheden die betrekking hebben tot hun weerbaarheid'), hetzij op een meer algemene manier."

De bepaling moet gewijzigd worden in de zin die door de gemachtigde van de Minister wordt aangegeven.

Bovendien dient, zoals de bedoeling lijkt te zijn van de steller van het voorontwerp, te worden verduidelijkt dat de delegatie aan de Koning houdende nadere bepaling van de coördinerende rol van de autoriteit bedoeld in artikel 21, § 1, eveneens slaat op het faciliteren van de vrijwillige informatie-uitwisseling tussen de kritieke entiteiten over aangelegenheden waarop het voorontwerp betrekking heeft.

Artikel 25

1. In tegenstelling tot wat in de bespreking van artikel 25 staat, voorziet dat artikel niet dat de inspectiedienst het recht krijgt op volledige of gedeeltelijke toegang tot het WPE.

De steller van het voorontwerp moet toezien op de samenhang tussen de bespreking van het artikel en het dispositief.

2. In de Franse tekst dient het woord "externe" ingevoegd te worden tussen het woord "protection" en de woorden "des entités critiques".

In de Nederlandse tekst dient men "externe bescherming" te schrijven in plaats van "weerbaarheid".

Articles 21, 27 et 28

Interrogé sur la correcte transposition de l'article 10, paragraphe 3, de la directive CER par les articles 21, § 3, 27 et 28, § 1er, de l'avant-projet, le délégué a expliqué ce qui suit:

"In principe zijn kritieke entiteiten gehouden aan de beperkte verspreiding en het beroepsgeheim. Volgens artikel 10 van de CER Richtlijn dient het faciliteren te gebeuren o.a. overeenkomstig het nationaal recht met betrekking tot gevoelige informatie. Daarnaast kan de Koning wel de coördinerende rol van het NCCN met betrekking tot de weerbaarheid van kritieke entiteiten verder uitwerken, inclusief het faciliteren van informatie delen tussen kritieke entiteiten, maar wel steeds rekening houdend met de behandeling van gevoelige informatie.

Onzes inziens valt het bepalen van duidelijke grenzen waarbinnen kritieke entiteiten vrijwillig informatie kunnen delen ook onder deze faciliterende taak, wat deze bepaling van het dispositief ook duidelijk beoogt.

Indien nodig, bestaat er een mogelijkheid om een verwijzing naar deze facilitatie-rol van het NCCN duidelijker op te nemen in het voorontwerp van wet, hetzij in de onderhavige bepaling ('In voorkomend geval, en wanneer zij van oordeel is dat dit opportuun is, kan de autoriteit bedoeld in art. 21, § 1, voorzien in de verdere facilitatie van het vrijwillig delen van informatie tussen kritieke entiteiten over aangelegenheden die betrekking hebben tot hun weerbaarheid'), hetzij op een meer algemene manier".

La disposition sera modifiée dans le sens indiqué par le délégué de la Ministre.

Par ailleurs, comme cela semble être la volonté de l'auteure de l'avant-projet, il conviendrait de clarifier que la délégation au Roi Lui permettant de préciser le rôle de coordination de l'autorité visée à l'article 21, § 1er, englobe également la facilitation du partage volontaire d'informations entre les entités critiques sur les questions couvertes par l'avant-projet.

Article 25

1. Contrairement à ce qu'indique son commentaire, l'article 25 ne prévoit pas le droit pour le service d'inspection d'accéder en tout ou en partie au P.R.E.

L'auteure de l'avant-projet veillera à assurer la cohérence entre le commentaire de l'article et le dispositif.

2. Dans la version française, il convient d'insérer le mot "externe" entre le mot "protection" et les mots "des entités critiques".

Dans la version néerlandaise, on écrira "externe bescherming" plutôt que "weerbaarheid".

Artikel 29

Aangezien de wet van 5 augustus 2006 ‘betreffende de toegang van het publiek tot milieu-informatie’ strekt tot omzetting van richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 ‘inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad’, is artikel 29 in strijd met het recht van de Europese Unie voor zover het stelt dat de wet van 2006 niet van toepassing is op informatie, documenten of gegevens, in welke vorm ook, bedoeld in artikel 27. Het moet op dat punt dan ook herzien worden.

Artikel 30

Op de vraag wie de in paragraaf 2 bedoelde bevoegde minister is, heeft de gemachtigde van de Minister het volgende geantwoord:

“Het betreft de bevoegde minister voor de welbepaalde sector of deelsector, zoals bepaald in de bijlage.”

Wat betreft de sectoren die onder de bevoegdheid van de deelstaten vallen, heeft de gemachtigde van de Minister eveneens de volgende verduidelijking gegeven:

“Voor deze sectoren zal de sectorale overheid bestaan uit een *sui generis* orgaan waarin alle bevoegde autoriteiten in vertegenwoordigd zijn. Aangezien de wetgeving met betrekking tot de weerbaarheid van kritieke entiteiten valt onder de federale bevoegdheid inzake nationale veiligheid, zal er ook altijd een federale administratie vertegenwoordigd zijn in deze sectorale overheid. Bijkomend betreft het de classificatie op grond van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, waarvoor de federale minister van Justitie bevoegd is.

Bijgevolg zullen de federaal bevoegde minister van de desbetreffende sector of deelsector, alsook de federale minister bevoegd voor de wetgeving betreffende de classificaties verantwoordelijk zijn voor het voordragen van de uitvoeringsbesluiten hieromtrent.”

De afdeling Wetgeving wijst de steller van het voorontwerp op het feit dat, zoals eerder aangegeven, de deelstaten bij het voorontwerp betrokken mogen worden, maar dan enkel zodanig dat de autonomie van de verschillende bevoegdheidsniveaus in acht genomen wordt. De federale wetgever kan deelstaten niet eenzijdig, bij wege van een gewone wet, dwingen mee te werken aan de regeling die wordt ingevoerd. Er kan zo nodig enkel voorzien worden in een facultatieve medewerking van de deelstaten, en wel zodanig dat hun eventuele onthouding niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen neemt.[13]

Artikel 30 moet in voorkomend geval herzien worden in het licht van deze opmerking.

[13] Zie advies 48.989/VR.

Article 29

Étant donné que la loi du 5 août 2006 ‘relative à l’accès du public à l’information en matière d’environnement’ transpose la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 ‘concernant l’accès du public à l’information en matière d’environnement et abrogeant la directive 90/313/CEE du Conseil’, l’article 29 entre en contrariété avec le droit de l’Union européenne en ce qu’il affirme que la loi du 5 août 2006 ne s’applique pas aux informations, documents ou données, sous quelque forme que ce soit, visés à l’article 27. Il sera dès lors revu sur ce point.

Article 30

Interrogé quant à savoir qui est le ministre compétent visé au paragraphe 2, le délégué de la Ministre a répondu ce qui suit:

“Het betreft de bevoegde minister voor de welbepaalde sector of deelsector, zoals bepaald in de bijlage”.

Concernant les secteurs relevant de la compétence des entités fédérées, le délégué de la Ministre a également précisé ce qui suit:

“Voor deze sectoren zal de sectorale overheid bestaan uit een *sui generis* orgaan waarin alle bevoegde autoriteiten in vertegenwoordigd zijn. Aangezien de wetgeving met betrekking tot de weerbaarheid van kritieke entiteiten valt onder de federale bevoegdheid inzake nationale veiligheid, zal er ook altijd een federale administratie vertegenwoordigd zijn in deze sectorale overheid. Bijkomend betreft het de classificatie op grond van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, waarvoor de federale minister van Justitie bevoegd is.

Bijgevolg zullen de federaal bevoegde minister van de desbetreffende sector of deelsector, alsook de federale minister bevoegd voor de wetgeving betreffende de classificaties verantwoordelijk zijn voor het voordragen van de uitvoeringsbesluiten hieromtrent”.

La section de législation attire l’attention de l’auteure de l’avant-projet sur le fait que, comme précédemment indiqué, si l’avant-projet peut impliquer les entités fédérées, il doit le faire d’une manière qui respecte l’autonomie des différents niveaux de pouvoir. Le législateur fédéral ne peut imposer unilatéralement, par le biais d’une loi ordinaire, une collaboration forcée des entités fédérées au système mis en place. L’intervention des entités fédérées ne peut être prévue, si nécessaire, que de façon facultative et en manière telle que leur éventuelle abstention n’empêche pas l’adoption des mesures envisagées par l’autorité fédérale compétente[13].

L’article 30 sera le cas échéant revu à la lumière de cette observation.

[13] Voir l’avis 48.989/VR.

Artikel 31

Paragraaf 1 bepaalt dat de Koning per sector of in voorkomend geval per deelsector een inspectiedienst aanstelt, en paragraaf 2 bepaalt dat de Koning de nadere regels voor de controle vastlegt.

Wat dat betreft, moet worden opgemerkt dat de bescherming van de persoonlijke levenssfeer en van de woning, die inzonderheid gewaarborgd wordt door artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet, onder meer betrekking kan hebben op vertrekken waarin beroeps- en handelsactiviteiten worden uitgeoefend.[14]

In dat verband heeft het Grondwettelijk Hof herinnerd aan "de ruime draagwijdte van het begrip 'woning'", al kan "de inmenging van de wetgever (…) groter zijn wanneer het gaat om beroeps- of handelsactiviteiten of om de ruimtes waar die activiteiten worden uitgeoefend (EHRM, 14 maart 2013, *Bernh Larsen Holding AS e.a. t. Noorwegen,* § 104; 16 december 1992, *Niemietz t. Duitsland*, § 31)."[15]

Het Grondwettelijk Hof heeft eveneens aan het volgende herinnerd:

"De rechten die bij de artikelen 15 en 22 van de Grondwet en bij artikel 8 van het Europees Verdrag voor de rechten van de mens worden gewaarborgd, vereisen dat elke overheidsinmenging in het recht op eerbiediging van het privéleven en van de woning wordt voorgeschreven in een voldoende precieze wettelijke bepaling, beantwoordt aan een dwingende maatschappelijke behoefte en evenredig is met de daarin nagestreefde wettige doelstelling."[16]

Een inmenging in het recht op de eerbiediging van de woning dient dan ook te worden afgebakend met bepaalde waarborgen en mag geen "algemeen, onvoorwaardelijk en onbeperkt recht van vrije toegang tot de beroepslokalen" inhouden. Zo heeft het Hof in arrest 116/2017 van 12 oktober 2017 geoordeeld dat "rekening houdend met wat in het bijzonder is vermeld in B.10.2 en B.11.3", de fiscale visitatie in kwestie voldoet aan de vereiste van voorzienbaarheid bedoeld in artikel 8.2 van het Europees Verdrag voor de rechten van de mens.[17] Het Hof hield er rekening mee dat de bepalingen in kwestie de bevoegde personeelsleden er niet toe machtigden inzage te eisen in de boeken en documenten in kwestie als de belastingplichtige zich daartegen verzet, en evenmin zich met dwang toegang te verschaffen tot de beroepslokalen indien de belastingplichtige zich daartegen verzet.

14 Zie met name advies 74.789/4 van 18 januari 2024 over een voorontwerp van decreet 'modifiant le Code de l'habitation durable ainsi que le décret du 18 mars 2002 relatif à l'Infrastructure' (*Parl. St.* D.Parl. 2023-24, nr. 331/1, 51-65) en advies 75.019/4 van 19 februari 2024 over een voorontwerp dat geleid heeft tot het decreet van 28 maart 2024 'over het vervoer van koolstofdioxide via pijpleidingen' (*Parl.St.* W.Parl. 2023-24, nr. 1639/1, 21-42).

15 GwH 20 juli 2023, nr. 113/2023, B.35.5 en B.36.2.

16 Ibidem, B.35.6.

17 GwH 12 oktober 2017, nr. 116/2017, B.12; zie ook GwH 27 juni 2019, nr. 104/2019, B.8.

Article 31

Le paragraphe 1er prévoit que le Roi institue un service d'inspection par secteur ou, le cas échéant, par sous-secteur et le paragraphe 2 habilite le Roi à fixer les modalités de contrôle.

Il y a lieu à cet égard de rappeler que la protection de la vie privée et du domicile, garantie notamment par l'article 8 de la Convention européenne des droits de l'homme et par l'article 22 de la Constitution, peut couvrir notamment des locaux où sont exercées des activités professionnelles et commerciales[14].

La Cour constitutionnelle a rappelé à cet égard "la portée étendue de la notion de 'domicile'", même si l'ingérence du législateur peut "être plus importante lorsqu'il s'agit de locaux ou d'activités professionnelles ou commerciales (CEDH, 14 mars 2013, *Bernh Larsen Holding AS e.a. c. Norvège*, § 104; 16 décembre 1992, *Niemietz c. Allemagne*, § 31)"[15].

La Cour constitutionnelle a également rappelé que

"[l]es droits que garantissent les articles 15 et 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme exigent que toute ingérence des autorités dans le droit au respect de la vie privée et du domicile soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit"[16].

Il convient dès lors qu'une ingérence dans le domicile soit encadrée de certaines garanties et ne confère pas "un droit général, inconditionnel et illimité de libre accès aux locaux professionnels". Ainsi, par son arrêt n° 116/2017 du 12 octobre 2017, la Cour a jugé, "compte tenu de ce qui est dit en particulier en B.10.2 et B.11.3", que la visite fiscale en cause satisfaisait à la condition de prévisibilité visée à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme[17]. La Cour tenait compte de ce que les dispositions en cause n'autorisaient pas les agents compétents à exiger la consultation des livres et documents en question si le contribuable s'y oppose, pas plus qu'elles ne leur permettaient de se procurer par la contrainte un accès aux locaux professionnels si le contribuable s'y oppose.

14 Voir notamment l'avis 74.789/4 donné 18 janvier 2024 sur un avant-projet de décret 'modifiant le Code de l'habitation durable ainsi que le décret du 18 mars 2002 relatif à l'Infrastructure' (*Doc. parl.*, Parl. D. Gem., 2023-2024, n° 331/1, pp. 51-65) et l'avis 75.019/4 donné le 19 février 2024 sur un avant-projet devenu le décret du 28 mars 2024 'relatif au transport de dioxyde de carbone par canalisations' (*Doc. parl.*, Parl. w., 2023-2024, n° 1639/1, pp. 21-42).

15 C.C., 20 juillet 2023, n° 113/2023, B.35.5 et B.36.2.

16 *Ibidem*, B.35.6.

17 C.C., 12 octobre 2017, n° 116/2017, B.12; voir aussi C.C., 27 juin 2019, n° 104/2019, B.8.

Evenzo heeft het Grondwettelijk Hof, bij arrest nr. 113/2023 van 20 juli 2023, geoordeeld dat de bepaling op grond waarvan gebouwen bestemd voor erediensten, met uitzondering van een privéwoning, "zonder voorafgaande aankondiging" mogen worden betreden, "het bijgevolg en *a fortiori* de bevoegde personeelsleden niet mogelijk [maakt] om zich met geweld of dwang toegang te verschaffen tot de gebouwen die bestemd zijn voor de uitoefening van de eredienst, tot de ruimtes en de infrastructuur die het bestuur van de eredienst gebruikt of die de lokale geloofsgemeenschap gebruikt tijdens de wachtperiode, indien de betrokkenen hun medewerking niet hebben verleend. De bevoegde personeelsleden kunnen evenmin de personen bestraffen die de toegang tot die gebouwen en ruimtes zouden weigeren, maar enkel daarvan melding maken in hun advies omtrent de toekenning van de erkenning" (B.36.3).

Door aan de bevoegde wetgever de bevoegdheid voor te behouden te bepalen in welke gevallen en onder welke voorwaarden het recht op eerbiediging van het privéleven kan worden aangetast, waarborgt artikel 22 van de Grondwet bovendien iedere burger dat geen enkele inmenging in dat recht toegelaten is dan krachtens de regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.[18] Zo voorziet artikel 22 van de Grondwet in een formele-legaliteitsvereiste voor elke inmenging in het recht op het privéleven.

Op de vraag waarom geopteerd is voor een delegatie aan de Koning, heeft de gemachtigde van de Minister het volgende geantwoord:

"Voor wat betreft de inspecties en audits werd gekozen voor een delegatie aan de Koning zodat elke sector of deelsector de nadere regels kan vastleggen, rekening houdend met de specificiteiten van hun sector of deelsector. Deze werkwijze houdt een voortzetting in van het huidige beleid inzake inspecties op grond van de wet van 1 juli 2011 en stemt overeen met de verplichting uit artikel 21, paragraaf 1, van de CER Richtlijn om te zorgen dat de bevoegde autoriteiten over bevoegdheden beschikken om inspecties en audits uit te voeren in de kritieke entiteit. De modaliteiten van het uitvoeren van inspecties wordt niet gespecifieerd in de CER Richtlijn waardoor gebruik werd gemaakt van deze opportuniteit om een delegatie te geven aan de Koning, zodat de regelgeving hieromtrent op (deel)sectoraal niveau kan worden opgesteld, waarbij tevens tegemoet werd gekomen aan de vraag hiertoe van de bevoegde sectorale overheden."

Gelet op het legaliteitsbeginsel dat ter zake van toepassing is, is de machtiging aan de Koning om de nadere regels vast te stellen voor de controle door de inspectiedienst niet toelaatbaar. De uitleg van de gemachtigde van de Minister doet niets af aan die vaststelling. De afdeling Wetgeving merkt in dat verband op dat de wet van 1 juli 2011 'betreffende de beveiliging en de bescherming van de kritieke infrastructuren' zelf voorzag in bepaalde bevoegdheden voor de inspectiedienst en een beperktere machtiging verleende aan de Koning.

[18] GwH 14 maart 2013, nr. 39/2013, B.8.1.

De même, la Cour constitutionnelle a, par son arrêt n° 113/2023 du 20 juillet 2023, jugé que la disposition permettant d'entrer "sans préavis" dans des lieux de cultes à l'exclusion d'un domicile privé "ne permet donc et à fortiori pas aux agents compétents d'accéder par la force ou par la contrainte aux bâtiments destinés à l'exercice du culte, aux locaux et aux infrastructures que l'administration du culte utilise ou à ceux que la communauté religieuse locale utilise pendant la période d'attente, si les intéressés ne coopèrent pas. Les agents compétents ne peuvent pas davantage sanctionner les personnes qui refuseraient l'accès à ces bâtiments et locaux, mais uniquement en faire mention dans leur avis sur l'octroi de la reconnaissance" (B.36.3)

Par ailleurs, en réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune immixtion dans ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue[18]. Ainsi, l'article 22 de la Constitution prévoit une exigence de légalité formelle pour toute ingérence dans le droit à la vie privée.

Interrogé sur les raisons pour lesquelles il a été opté pour une délégation au Roi, le délégué de la Ministre a répondu ce qui suit:

"Voor wat betreft de inspecties en audits werd gekozen voor een delegatie aan de Koning zodat elke sector of deelsector de nadere regels kan vastleggen, rekening houdend met de specificiteiten van hun sector of deelsector. Deze werkwijze houdt een voortzetting in van het huidige beleid inzake inspecties op grond van de wet van 1 juli 2011 en stemt overeen met de verplichting uit artikel 21, paragraaf 1, van de CER Richtlijn om te zorgen dat de bevoegde autoriteiten over bevoegdheden beschikken om inspecties en audits uit te voeren in de kritieke entiteit. De modaliteiten van het uitvoeren van inspecties wordt niet gespecifieerd in de CER Richtlijn waardoor gebruik werd gemaakt van deze opportuniteit om een delegatie te geven aan de Koning, zodat de regelgeving hieromtrent op (deel)sectoraal niveau kan worden opgesteld, waarbij tevens tegemoet werd gekomen aan de vraag hiertoe van de bevoegde sectorale overheden".

Compte tenu du principe de légalité applicable en la matière, l'habilitation au Roi pour fixer les modalités du contrôle opéré par le service d'inspection n'est pas admissible. L'explication fournie par le délégué de la Ministre ne modifie en rien ce constat. La section de législation remarque à cet égard que la loi du 1er juillet 2011 'relative à la sécurité et la protection des infrastructures critiques' prévoyait elle-même certains pouvoirs du service d'inspection et octroyait une délégation plus limitée au Roi.

[18] C.C., 14 mars 2013, n° 39/2013, B.8.1.

Het dispositief moet aangevuld worden in het licht van deze opmerking, in voorkomend geval naar het voorbeeld van het bepaalde in artikel 48 van de NIS 2-wet.

Artikel 33

1. De eerste zin van paragraaf 2 bepaalt het volgende:

"De inspectiedienst kan de overtreder vooraf, op een met redenen omklede wijze, meedelen dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord."

Ingeval de inspectiedienst de overtreder niet meedeelt dat hij van plan is hem een ingebrekestelling te sturen, kan de overtreder zijn verweermiddelen dan ook niet schriftelijk indienen, noch vragen om te worden gehoord.

Op een vraag in dat verband heeft de gemachtigde van de Minister het volgende geantwoord:

"De wetgeving betreffende de weerbaarheid van kritieke entiteiten steunt op onderlinge samenwerking en overleg tussen de bevoegde autoriteiten en de betrokken kritieke entiteiten. Daarom werd er gekozen om, vooraf aan de ingebrekestelling, de mogelijkheid te geven tot gemotiveerde mededeling betreffende de vastgestelde inbreuk.

Voorstel om deze bepaling te harmoniseren met de NIS 2-wet door een uitzondering toe te voegen, waardoor het duidelijker wordt dat het een verplichting betreft waarvan enkel kan afgeweken worden in bepaalde gevallen.

'In afwijking van het eerste lid wordt dergelijke gemotiveerde mededeling niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd'."

De afdeling Wetgeving kan instemmen met het voorstel van de gemachtigde. Paragraaf 2 moet evenwel worden gewijzigd om nader te bepalen dat de inspectiedienst, behoudens behoorlijk gemotiveerde uitzonderingen, vooraf moet meedelen dat hij van plan is de overtreder een ingebrekestelling te sturen en hem moet laten weten dat deze het recht heeft om binnen een termijn van dertig dagen zijn verweermiddelen in te dienen of om te vragen te worden gehoord.

2. Op de vraag of de steller van het voorontwerp met de woorden "De informatie wordt geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de inspectiedienst" in paragraaf 2 het bestaan van een weerlegbaar dan wel een onweerlegbaar vermoeden heeft willen opnemen, heeft de gemachtigde van de Minister het volgende geantwoord:

Le dispositif sera complété à la lumière de l'observation, à l'instar, le cas échéant, de ce que prévoit l'article 48 de la loi NIS 2.

Article 33

1. La première phrase du paragraphe 2 prévoit que

"[l]e service d'inspection peut notifier préalablement au contrevenant, de manière motivée, son intention de lui adresser une mise en demeure et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de cette information, de présenter ses moyens de défense par écrit ou de demander à être entendu".

Ainsi, en l'absence de notification au contrevenant par le service d'inspection de son intention de lui adresser une mise en demeure, le contrevenant ne peut présenter ses moyens de défense par écrit ou demander à être entendu.

Interrogé sur ce point, le délégué de la Ministre a indiqué ce qui suit:

"De wetgeving betreffende de weerbaarheid van kritieke entiteiten steunt op onderlinge samenwerking en overleg tussen de bevoegde autoriteiten en de betrokken kritieke entiteiten. Daarom werd er gekozen om, vooraf aan de ingebrekestelling, de mogelijkheid te geven tot gemotiveerde mededeling betreffende de vastgestelde inbreuk.

Voorstel om deze bepaling te harmoniseren met de NIS 2-wet door een uitzondering toe te voegen, waardoor het duidelijker wordt dat het een verplichting betreft waarvan enkel kan afgeweken worden in bepaalde gevallen.

'In afwijking van het eerste lid wordt dergelijke gemotiveerde mededeling niet vooraf naar de betrokken entiteit gestuurd in naar behoren gemotiveerde uitzonderlijke gevallen waarin een onmiddellijk optreden om een incident te voorkomen of erop te reageren anders zou worden belemmerd'".

La section de législation peut se rallier à la proposition du délégué. Le paragraphe 2 devra toutefois être modifié pour préciser que le service d'inspection doit, sauf exceptions dûment justifiées, notifier préalablement son intention d'adresser une mise en demeure au contrevenant et l'informer qu'il a le droit de présenter ses moyens de défense ou de demander à être entendu dans un délai de trente jours.

2. Interrogé sur la question de savoir si, au paragraphe 2, en utilisant les termes "L'information est réputée avoir été reçue par le contrevenant le sixième jour après son envoi par le service d'inspection", l'auteure de l'avant-projet entend instituer une présomption réfragable ou irréfragable, le délégué de la Ministre a répondu ce qui suit:

"Het betreft een weerlegbaar vermoeden. Suggestie om ter verduidelijking toe te voegen in het dispositief: 'behoudens tegenbewijs'."

Het dispositief moet in die zin aangevuld worden. De opmerking geldt *mutatis mutandis* voor artikel 40.

Artikelen 33 tot 40

1. Artikel 34 legt de inspectiedienst de verplichting op om het origineel van het proces-verbaal waarin wordt vastgesteld dat de kritieke entiteit binnen de vastgestelde termijn geen gevolg heeft gegeven aan de ingebrekestelling inzake het voldoen van haar wettelijke verplichtingen, naar de procureur des Konings te sturen. De bepaling lijkt zodoende van toepassing te zijn op alle gevallen waarin sprake is van inbreuken op de voorschriften van de wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen.[19]

Artikel 36 bepaalt dat de procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging is ingesteld. De procedure voor het opleggen van een administratieve geldboete mag niet worden opgestart voordat die termijn is verstreken, behalve wanneer de procureur des Konings vooraf meedeelt dat hij geen gevolg aan de inbreuk wenst te geven.

Artikel 38 bepaalt in welke gevallen een strafrechtelijke sanctie kan worden opgelegd, alsook de strafmaat. Paragraaf 1 bepaalt dat een dergelijke sanctie enkel kan worden opgelegd indien de kritieke entiteiten de maatregelen niet in acht nemen die door hoofdstuk 2 en hoofdstuk 4, afdeling 2, van het voorontwerp worden voorgeschreven, terwijl uit paragraaf 2 voortvloeit dat een strafrechtelijke sanctie ook zou kunnen worden opgelegd aan "eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt".

Meer in het algemeen voorziet artikel 39 in de mogelijkheid een administratieve sanctie op te leggen voor "elke inbreuk" op deze wet, op de uitvoeringsbesluiten ervan of op de administratieve beslissingen die krachtens deze wet genomen worden.

2. De gemachtigde van de minister is gevraagd:

(i) waarom administratieve sancties worden voorzien;

(ii) waarom de administratieve sancties worden voorzien in ruimer omschreven gevallen dan die waarop de strafrechtelijke sancties betrekking hebben;

(iii) waarom de administratieve sancties hoger zijn dan de strafrechtelijke sancties.

[19] Dat volgt immers uit artikel 33 van het voorontwerp.

"Het betreft een weerlegbaar vermoeden. Suggestie om ter verduidelijking toe te voegen in het dispositief: 'behoudens tegenbewijs'".

Le dispositif sera complété en ce sens, l'observation valant *mutatis mutandis*, pour l'article 40.

Articles 33 à 40

1. L'article 34 impose l'obligation au service d'inspection d'envoyer au Procureur du Roi l'original du procès-verbal dans lequel il est constaté que l'entité critique, mise en demeure de remplir ses obligations légales, ne s'est pas exécutée dans le délai imparti. La disposition se présente ainsi comme s'appliquant à toutes les hypothèses d'infractions aux exigences de la loi, de ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes[19].

L'article 36 prévoit que le Procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour informer l'autorité sectorielle que des poursuites pénales ont été engagées. La procédure d'imposition d'une amende administrative ne peut être entamée avant l'expiration de ce délai, à moins que le Procureur du Roi ne notifie préalablement qu'il ne souhaite pas donner suite à l'infraction.

L'article 38 détermine les cas dans lesquels une sanction pénale peut être infligée ainsi que le taux de la peine. Le paragraphe 1er prévoit que seul le non-respect, par les entités critiques, des mesures prescrites par le chapitre 2 et le chapitre 4, section 2, de l'avant-projet peut entraîner l'infliction d'une sanction de cette nature, tandis qu'il ressort du paragraphe 2 qu'une sanction pénale pourrait également être infligée à "quiconque empêche ou entrave volontairement l'exécution du contrô1e effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrô1e, ou communique sciemment des informations inexactes ou incomplètes".

Plus largement, l'article 39 prévoit la possibilité d'infliger une sanction administrative pour "toute violation" de la loi, de ses arrêtés d'exécution ou des décisions administratives prise en exécution de la loi.

2. Interrogé sur les raisons pour lesquelles

(i) des sanctions administratives sont prévues

(ii) les sanctions administratives sont prévues dans des cas plus étendus que ceux visés par les sanctions pénales

(iii) les sanctions administratives sont plus élevées que les sanctions pénales,

[19] Cela résulte en effet de l'article 33 de l'avant-projet.

De gemachtigde van de Minister heeft het volgende geantwoord:

“Met betrekking tot (i): administratieve sancties werden voorzien in het voorontwerp om drie redenen:

o 1° Harmonisatie met het wetgevend kader uit de NIS 1 en NIS 2 wetten. CER en NIS kunnen niet los van elkaar gezien worden.

o 2° Op verzoek van de betrokken sectorale overheden: in het huidig wetgevend kader werden enkel strafrechtelijke sancties voorzien, hetgeen als niet voldoende werd geacht door de sectorale overheden. De strafrechtelijke sancties werden in de praktijk nooit gebruikt aangezien de sectorale overheden hiervoor zelf niet bevoegd zijn, maar langs de procureur des Konings moeten gaan. Kleine inbreuken bleven bijgevolg onbestraft.

o 3° Om discriminatie tussen de verschillende sectoren te voorkomen: sommige sectoren kunnen op basis van andere sectorale wetgeving administratieve sancties opleggen, anderen niet. Door in het voorontwerp de mogelijkheid te schrijven tot het opleggen van administratieve sancties, bestaat voor elke sector nu deze mogelijkheid.

Met betrekking tot (ii): het opleggen van administratieve sancties is voor wat betreft de materie van het voorontwerp vaak efficiënter en effectiever dan het opleggen van strafrechtelijke sancties. Het doel van sancties te voorzien is om een drukkingsmiddel ter beschikking te hebben wanneer nodig, d.w.z. dat de sancties ook effectief opgelegd worden. De toevoeging van administratieve sancties zorgt ervoor dat, wanneer de Procureur des Konings beslist om geen strafrechtelijke vervolging in te stellen, de sectorale overheid alsnog een administratieve sanctie kan opleggen aan de overtreder. Het risico bestaat dat een overtreding van deze wetgeving door de procureur des Konings niet als prioriteit wordt geacht om een strafrechtelijke vervolging tegen in te stellen. Het toepassingsgebied werd uitgebreid ten opzichte van de strafrechtelijke sancties aangezien de strafrechtelijke sancties zich voornamelijk focussen op zwaardere inbreuken.

Met betrekking tot (iii): bij de strafrechtelijke sancties riskeert men een gevangenisstraf, waarbij beargumenteerd kan worden dat dit zwaarder is dan enige geldboete. Voor de administratieve boetes werd er voorzien in een ruime beslissingsmarge voor de hoogte van de geldboetes, hetgeen beslist kan worden aan de hand van de ernst van de inbreuk. Het maximumbedrag ligt inderdaad hoger, mede gelet op het feit dat er geen gevangenisstraf bij komt kijken, maar het minimumbedrag ligt eveneens lager dan bij de strafrechtelijke sancties. Aangezien kritieke entiteiten ook automatisch als essentiële entiteiten worden aanzien onder de NIS 2 wet werden de bedragen van de administratieve sancties geharmoniseerd met de bedragen van de administratieve sancties die worden voorzien in de NIS 2 wet.”

3. De aldus opgevatte sanctieprocedure geeft aanleiding tot verschillende opmerkingen.

le délégué de la Ministre a répondu ce qui suit:

“Met betrekking tot (i): administratieve sancties werden voorzien in het voorontwerp om drie redenen:

o 1° Harmonisatie met het wetgevend kader uit de NIS 1 en NIS 2 wetten. CER en NIS kunnen niet los van elkaar gezien worden.

o 2° Op verzoek van de betrokken sectorale overheden: in het huidig wetgevend kader werden enkel strafrechtelijke sancties voorzien, hetgeen als niet voldoende werd geacht door de sectorale overheden. De strafrechtelijke sancties werden in de praktijk nooit gebruikt aangezien de sectorale overheden hiervoor zelf niet bevoegd zijn, maar langs de procureur des Konings moeten gaan. Kleine inbreuken bleven bijgevolg onbestraft.

o 3° Om discriminatie tussen de verschillende sectoren te voorkomen: sommige sectoren kunnen op basis van andere sectorale wetgeving administratieve sancties opleggen, anderen niet. Door in het voorontwerp de mogelijkheid te schrijven tot het opleggen van administratieve sancties, bestaat voor elke sector nu deze mogelijkheid.

Met betrekking tot (ii): het opleggen van administratieve sancties is voor wat betreft de materie van het voorontwerp vaak efficiënter en effectiever dan het opleggen van strafrechtelijke sancties. Het doel van sancties te voorzien is om een drukkingsmiddel ter beschikking te hebben wanneer nodig, d.w.z. dat de sancties ook effectief opgelegd worden. De toevoeging van administratieve sancties zorgt ervoor dat, wanneer de Procureur des Konings beslist om geen strafrechtelijke vervolging in te stellen, de sectorale overheid alsnog een administratieve sanctie kan opleggen aan de overtreder. Het risico bestaat dat een overtreding van deze wetgeving door de procureur des Konings niet als prioriteit wordt geacht om een strafrechtelijke vervolging tegen in te stellen. Het toepassingsgebied werd uitgebreid ten opzichte van de strafrechtelijke sancties aangezien de strafrechtelijke sancties zich voornamelijk focussen op zwaardere inbreuken.

Met betrekking tot (iii): bij de strafrechtelijke sancties riskeert men een gevangenisstraf, waarbij beargumenteerd kan worden dat dit zwaarder is dan enige geldboete. Voor de administratieve boetes werd er voorzien in een ruime beslissingsmarge voor de hoogte van de geldboetes, hetgeen beslist kan worden aan de hand van de ernst van de inbreuk. Het maximumbedrag ligt inderdaad hoger, mede gelet op het feit dat er geen gevangenisstraf bij komt kijken, maar het minimumbedrag ligt eveneens lager dan bij de strafrechtelijke sancties. Aangezien kritieke entiteiten ook automatisch als essentiële entiteiten worden aanzien onder de NIS 2 wet werden de bedragen van de administratieve sancties geharmoniseerd met de bedragen van de administratieve sancties die worden voorzien in de NIS 2 wet”.

3. La procédure de sanction ainsi conçue appelle plusieurs observations.

1° Doordat de procedure voorziet in het versturen van het door de inspectiedienst opgestelde proces-verbaal aan de procureur des Konings, wordt de onafhankelijkheid van het openbaar ministerie bij het uitoefenen van individuele onderzoeken en vervolgingen nageleefd.

In advies 72.195/2/AV van 12 december 2022 heeft de algemene vergadering van de afdeling Wetgeving in dat verband immers in herinnering gebracht dat de gerechtelijke overheden, en meer bepaald die welke onder het openbaar ministerie vallen, "prioritair de controle moeten behouden over de strafrechtelijke vervolgingen, gelet op de onafhankelijkheid die hun door artikel 151, § 1, van de Grondwet wordt gewaarborgd".[20]

Aangezien echter alleen de inbreuken bedoeld in artikel 38, §§ 1 en 2, tot een strafrechtelijke sanctie aanleiding kunnen geven, kan de verplichting, opgelegd in artikel 36, § 2, om het openbaar ministerie in te lichten, enkel voor deze inbreuken gelden, en dit ter wille van de inachtneming van de aldus in herinnering gebrachte beginselen.

2° Artikel 35 vermeldt dat inbreuken op deze wet of de uitvoeringsbesluiten ervan aanleiding kunnen geven tot strafrechtelijke of administratieve sancties.

In advies 74.284/3, van 5 oktober 2023[21] heeft de afdeling Wetgeving het volgende opgemerkt:

"Tot slot wenst de Raad van State, afdeling Wetgeving, er in dit verband op te wijzen dat een helder handhavingsbeleid wenselijk is. Het uitgangspunt is weliswaar de ruime keuzebevoegdheid van de wetgever, zowel inzake de definiëring van de inbreuken als inzake de passende afhandelingswijzen, uiteraard rekening houdend met de beginselen die met de keuze voor een strafrechtelijke of administratieve afhandeling gepaard gaan. Wel is het aan te raden dat de wetgever in dat kader eerst overweegt welke inbreuken op welke wijze te handhaven zijn, en dus niet zomaar alle inbreuken voor alle wijzen van handhaving (transactie, administratieve sanctie of strafsanctie) openstelt. In het bijzonder zou de wetgever moeten oordelen welke inbreuken louter administratief dan wel louter strafrechtelijk beantwoord moeten worden. Indien er daarbij een "tussenzone" wordt gecreëerd waarbij zowel administratieve als strafrechtelijke afhandeling mogelijk is, is het raadzaam een 'una via'-regeling te creëren, die inhoudt dat op een bepaald moment een keuze wordt gemaakt – met inachtneming van de zo-even geschetste mogelijkheid tot

[20] Advies 72.195/2/AV van 12 december 2022 over een voorontwerp dat geleid heeft tot de wet van 15 januari 2024 'betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen', opmerking 39 (*Parl.St.* Kamer 2022-23, nr. 1352/001, 141).

[21] Advies 74.284/3 van 5 oktober 2023 over een voorontwerp van wet 'betreffende de strafrechtelijke en administratieve sancties betreffende de inbreuken op sommige bepalingen van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt, van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen, van de wet van [11 juli 2023] betreffende het vervoer van waterstof door middel van leidingen en van hun uitvoeringsbesluiten'.

1° En tant qu'elle prévoit l'envoi au Procureur du Roi du procès-verbal dressé par le service d'inspection, la procédure s'inscrit dans le respect de l'indépendance du Ministère public dans l'exercice des recherches et poursuites individuelles.

À ce propos en effet, dans son avis 72.195/2/AG du 12 décembre 2022, l'assemblée générale de la section de législation a rappelé que "les autorités judiciaires, plus spécialement celles relevant du ministère public, doivent conserver la priorité de la maîtrise des poursuites pénales compte tenu des garanties d'indépendance qui leur sont reconnues par l'article 151, § 1er, de la Constitution"[20].

Compte tenu toutefois de ce que seules les infractions visées à l'article 38, §§ 1er et 2, sont susceptibles d'entraîner une sanction pénale, l'obligation d'information du Ministère public prescrite par l'article 36, § 2, n'est pertinente qu'à l'égard de ces seules infractions pour assurer le respect des principes ainsi rappelés.

2° L'article 35 énonce que les violations de la loi ou de ses arrêtés d'exécution peuvent donner lieu à des sanctions pénales ou administratives.

Dans l'avis 74.284/3 donné le 5 octobre 2023[21], la section de législation a observé ce qui suit:

"Enfin, le Conseil d'État, section de législation, tient à souligner à cet égard qu'une politique d'application de la loi transparente est souhaitable. La règle est certes que le législateur dispose d'un large pouvoir de choix, tant en ce qui concerne la définition des infractions que les modes de traitement adéquats, en tenant compte, bien entendu, des principes liés au choix d'un traitement pénal ou administratif. Il est toutefois conseillé que, dans ce contexte, le législateur envisage d'abord quelles infractions doivent être réprimées et de quelle manière, et qu'il n'ouvre donc pas purement et simplement toutes les infractions à tous les modes de répression (transaction, sanction administrative ou sanction pénale). En particulier, le législateur devrait apprécier quelles infractions devraient faire l'objet d'une réponse purement administrative ou purement pénale. Si, dans ce cadre, il est créé une 'zone intermédiaire' permettant un traitement tant administratif que pénal, il est conseillé de créer une règle *una via*, qui implique qu'à un moment donné, un choix est opéré – en tenant compte de la possibilité précitée de poursuites par le ministère public

[20] Avis 72.195/2/AG donné le 12 décembre 2022 sur un avant-projet devenu la loi du 15 janvier 2024 'relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les Pouvoirs publics', observation n° 39 (*Doc. parl.*, Chambre, 2022-2023, n° 1352/001, p. 141)

[21] Avis 74.284/3 donné le 5 octobre 2023 sur un avant-projet de loi "relative aux sanctions pénales et administratives concernant les infractions à certaines dispositions de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisation, de la loi du relatif au transport d'hydrogène par canalisations et de leurs arrêtés d'exécution".

vervolging door het openbaar ministerie – inzake de *in concreto* passende afhandelingswijze, die tot gevolg heeft dat de andere afhandelingswijze niet meer mogelijk is."

Voor zover administratieve sancties betrekking kunnen hebben op gevallen waarop ook strafrechtelijke sancties van toepassing zijn,[22] is de bovenstaande opmerking *mutatis mutandis* in dit geval van toepassing.

3° De strafmaat van de strafrechtelijke en administratieve sancties wordt vastgesteld in de artikelen 38 en 39.

Het belemmeren van of het niet meewerken aan het onderzoek van de inspectiedienst, bijvoorbeeld, kan krachtens artikel 38, § 2, worden bestraft met een gevangenisstraf van acht dagen tot een maand en een geldboete van 26 euro tot 1.000 euro, maar kan ook aanleiding geven tot een administratieve geldboete van 500 tot 125.000 euro.

Met betrekking tot de inachtneming van het gelijkheids- en evenredigheidsbeginsel ingeval de wetgever de strafrechtelijke of administratieve strafmaat vaststelt, heeft de afdeling Wetgeving in advies 74.284/3 as volgt gewezen op de adviespraktijk van de Raad van State en de rechtspraak van het Grondwettelijk Hof ter zake:

"Het gelijkheidsbeginsel impliceert dat voor de gelijke behandeling van onvergelijkbare gevallen een redelijke verantwoording voorhanden moet zijn, terwijl het evenredigheidsbeginsel inhoudt dat straffen proportioneel moeten zijn ten opzichte van de ernst van de inbreuk.[23] De afdeling Wetgeving heeft in het verleden reeds opgemerkt dat het beginsel van de evenredigheid van de straffen niet alleen voor de rechter, maar ook voor de wetgever geldt.[24] Het geldt overigens zowel ten aanzien van strafrechtelijke als administratieve sancties.[25] Volgens het Grondwettelijk Hof maakt het beginsel van de evenredigheid van de straffen 'integraal deel uit van ons rechtssysteem dat in de regel de rechter in staat stelt de straf te kiezen tussen een minimum en een maximum, hem ertoe machtigt rekening te houden met verzachtende omstandigheden en maatregelen van uitstel en opschorting van de uitspraak te bevelen, waardoor de rechter aldus in zekere mate de straf kan individualiseren door de straf op te leggen die hij evenredig acht met het geheel van de elementen van de zaak.'[26] Het Grondwettelijk Hof merkte op dat, niettegenstaande de 'beoordeling van de ernst van een misdrijf en van de strengheid waarmee het misdrijf kan worden bestraft, (…) tot de beoordelingsbevoegdheid van de wetgever [behoort]', het Hof bij de vraag naar de evenredigheid

[22] Dat blijkt in het bijzonder uit de artikelen 38, § 2, en 39, § 5, tweede lid, van het voorontwerp.

[23] *Voetnoot 25 van het geciteerde advies*: Zie o.m. adv.RvS 69.974/1V over een voorontwerp dat het decreet van 4 februari 2022 'tot wijziging van de wet van 14 augustus 1986 betreffende de bescherming en het welzijn der dieren, wat betreft het voorzien van een strafverzwaring' is geworden, opm. 3.1.

[24] *Voetnoot 26 van het geciteerde advies:* Zie o.m. adv.RvS 60.893/3 van 27 maart 2017 over een voorontwerp van 'Strafwetboek - Boek I', opm. 12.

[25] *Voetnoot 27 van het geciteerde advies:* GwH 18 februari 2016, nr. 25/2016, B.23.2.

[26] *Voetnoot 28 van het geciteerde advies:* GwH 22 december 2022, nr. 170/2022, B.24.2.

– concernant le mode de traitement adéquat *in concreto*, impliquant que l'autre mode de traitement n'est plus possible".

Dans la mesure où les sanctions administratives peuvent couvrir des hypothèses également visées par les sanctions pénales[22], l'observation qui précède vaut *mutatis mutandis* en l'espèce.

3° Le taux des sanctions pénales et administratives est fixé aux articles 38 et 39.

S'agissant, par exemple, de l'entrave ou de la non-collaboration à l'enquête du service d'inspection, celle-ci est punissable d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 à 1000 euros en vertu de l'article 38, § 2, tandis qu'elle peut être sanctionnée administrativement d'une amende pouvant aller de 500 à 125000 euros.

Concernant le respect du principe d'égalité et de proportionnalité lorsque le législateur fixe le taux d'une sanction, qu'elle soit pénale ou administrative, la section de législation dans l'avis 74.284/3 a rappelé comme suit la légisprudence du Conseil d'État et la jurisprudence de la Cour constitutionnelle en la matière:

"Le principe d'égalité implique que le traitement égal de cas non comparables doit pouvoir trouver une justification raisonnable, tandis que le principe de proportionnalité emporte que les peines doivent être proportionnées à la gravité de l'infraction[23]. Par le passé, la section de législation a déjà observé que le législateur, tout autant que le juge, doit avoir égard au principe de proportionnalité des peines[24]. Au demeurant, ce principe s'applique aux sanctions aussi bien pénales qu'administratives[25]. Selon la Cour constitutionnelle, le principe de la proportionnalité des peines 'fait également partie intégrante de notre système juridique qui, en règle, permet au juge de choisir la peine entre un minimum et un maximum, de tenir compte de circonstances atténuantes et d'ordonner le sursis et la suspension du prononcé, le juge pouvant ainsi individualiser la peine dans une certaine mesure, en infligeant celle qu'il estime proportionnée à l'ensemble des éléments de la cause'[26]. La Cour constitutionnelle a observé que, bien que l''appréciation de la gravité d'une infraction et de la sévérité avec laquelle l'infraction peut être punie relève du pouvoir d'appréciation du législateur', en s'interrogeant sur la proportionnalité des sanctions pénales instaurées, elle apprécie les 'cas dans lesquels le choix du législateur aboutit à traiter

[22] Ce qui ressort particulièrement des articles 38, § 2, et 39, § 5, alinéa 2, de l'avant-projet.

[23] *Note de bas de page n° 25 de l'avis cité*: Voir notamment l'avis C.E. 69.974/1V sur un avant-projet devenu le décret du 4 février 2022 'modifiant la loi du 14 août 1986 relative à la protection et au bien-être des animaux, en ce qui concerne la mise à disposition d'une aggravation de la sanction', observation 3.1.

[24] *Note de bas de page n° 26 de l'avis cité*: Voir entre autres l'avis C.E. 60.893/3 du 27 mars 2017 sur un avant-projet de 'Code pénal – Livre Premier', observation 12.

[25] *Note de bas de page n° 27 de l'avis cité*: C.C., 18 février 2016, n° 25/2016, B.23.2.

[26] *Note de bas de page n° 28 de l'avis cité*: C.C., 22 décembre 2022, n° 170/2022, B.24.2.

van de ingevoerde strafsancties een beoordeling vormt van ‘die gevallen waar de keuze van de wetgever leidt tot een kennelijk onredelijk verschil in behandeling tussen vergelijkbare misdrijven, of tot onevenredige gevolgen, gelet op de door de wetgever nagestreefde doelstellingen’.[27]”

Rekening houdend met de zonet in herinnering gebrachte beginselen moet het voorontwerp verder worden onderzocht om na te gaan of de opgelegde straffen in verhouding staan tot het nagestreefde doel. De memorie van toelichting moet worden aangevuld met een verantwoording ter zake.[28]

Artikel 34

In de Franse tekst van de onderzochte bepaling wordt nu eens over “rapport officiel” en dan weer over “procès-verbal” gesproken om naar hetzelfde document te verwijzen. De bepaling moet op dat punt geharmoniseerd worden.

Artikel 36

In de bespreking van het artikel wordt gesteld dat “[d]e dag van ontvangst wordt geacht de derde dag te zijn die volgt op deze waarop het kopie van het proces-verbaal aan de postdiensten overhandigd werd, tenzij de geadresseerde het tegendeel bewijst”. Die precisering zou in het dispositief opgenomen moeten worden.

Artikelen 38 en 39

1. In artikel 38, § 1, moeten de verwijzingen naar de hoofdstukken worden herzien. De interne weerbaarheidsmaatregelen staan immers in hoofdstuk 5 en de uitwisseling van informatie in hoofdstuk 6, afdeling 2.

2. Artikel 38, § 2, voorziet strafrechtelijke sancties voor eenieder die de uitvoering van de controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem naar aanleiding van deze controle wordt gevraagd weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt.

Het spreekt vanzelf dat die bepaling niet zo kan worden geïnterpreteerd dat een persoon tegen wie een vervolging is ingesteld, kan worden bestraft omdat hij geweigerd heeft zijn medewerking te verlenen bij het bewijzen van zijn eigen

de manière manifestement déraisonnable des infractions comparables ou à produire des effets disproportionnés, eu égard aux objectifs poursuivis par le législateur’[27]”.

Compte tenu des principes qui viennent d’être rappelés, l’avant-projet sera soumis à un examen complémentaire s’agissant d’apprécier le caractère proportionné des peines infligées au regard de l’objectif poursuivi. L’exposé des motifs sera complété par une justification en la matière[28].

Article 34

La version française de la disposition examinée évoque tantôt le rapport officiel tantôt le procès-verbal pour viser le même document. Elle sera harmonisée sur ce point.

Article 36

Le commentaire de l’article selon lequel “[l]e jour de réception est réputé être le troisième jour suivant celui où la copie du procès-verbal a été remise aux services postaux, sauf preuve contraire apportée par le destinataire” gagnerait à figurer dans le dispositif.

Articles 38 et 39

1. À l’article 38, § 1er, les renvois aux chapitres seront revus. En effet, les mesures internes de résilience sont prévues au chapitre 5 et l’échange d’informations au chapitre 6, section 2.

2. L’article 38, § 2, prévoit des sanctions pénales pour quiconque empêche ou entrave volontairement l’exécution du contrôle effectué par les membres du service d’inspection, refuse de communiquer les informations qui lui sont demandées à l’occasion de ce contrôle ou communique sciemment des informations inexactes ou incomplètes.

Il va de soi que cette disposition ne pourrait être interprétée comme impliquant qu’une personne pénalement accusée puisse être sanctionnée pour avoir refusé de prêter son concours à l’établissement de sa propre culpabilité puisque

27 *Voetnoot 29 van het geciteerde advies:* GwH 20 oktober 2022, nr. 134/2022, B.10.2. Ook ten aanzien van de in artikel 4, § 1, 4°, van het voorontwerp vermelde bepalingen van de verordening 2017/1938 geldt krachtens artikel 14, lid 10, van die verordening de verplichting in hoofde van de lidstaten om te voorzien in sancties die “doeltreffend, evenredig en afschrikkend” zijn.

28 Artikel 40, § 4, van het voorontwerp, waarin staat dat de administratieve geldboete in verhouding moet staan tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten, lijkt in dat opzicht ontoereikend te zijn.

27 *Note de bas de page n° 29 de l’avis cité*: C.C., 20 octobre 2022, n° 134/2022, B.10.2. L’obligation de prévoir des sanctions effectives, proportionnées et dissuasives imposée aux États membres en vertu de l’article 14, paragraphe 10, du règlement 2017/1938, s’applique aussi aux dispositions de ce règlement mentionnées à l’article 4, § 1er, 4°, de l’avant-projet.

28 L’article 40, § 4, de l’avant-projet, en ce qu’il énonce que l’amende administrative est proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de l’infraction, n’apparaît pas suffisant à cet égard.

schuld. Het recht om zichzelf niet te beschuldigen wordt immers gewaarborgd door artikel 14 , lid 3, g), van het Internationaal Verdrag inzake burgerrechten en politieke rechten en door artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens.[29]

Het Europees Hof voor de rechten van de mens erkent weliswaar uitzonderingen op dit verbod om "rechtstreekse dwang" uit te oefenen ten aanzien van het recht om zichzelf niet te beschuldigen, maar die uitzonderingen worden beperkend opgevat.[30]

Artikel 38, § 2, is dan ook enkel toelaatbaar in gevallen waarin de verplichting om de gevraagde informatie mee te delen, niet kan leiden tot een aantasting van het recht het stilzwijgen te bewaren.

Dezelfde opmerking geldt voor artikel 39, § 5, waarin wordt voorzien in administratieve sancties met een strafrechtelijk karakter in geval van niet-naleving van de verplichtingen betreffende de uitvoering van inspecties en audits, en voor eenieder die de uitvoering van de controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, die informatie die hem naar aanleiding van deze controle wordt gevraagd, weigert mee te delen, of die opzettelijk foutieve of onvolledige informatie meedeelt.

Artikelen 38 en 40

Het voorontwerp bevat bepalingen in verband met de verhoging van de sanctie in geval van recidive.

Zo bepaalt artikel 38, § 1, tweede lid, dat de geldboete wordt verdubbeld en de overtreder wordt gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.[31] Er wordt ook voorzien in strafverzwaring in geval van herhaling van de inbreuk die bij artikel 38, § 2, strafrechtelijk wordt bestraft. De administratieve geldboete wordt krachtens artikel 40, § 4, tweede lid, ook verdubbeld "in geval van herhaling binnen een termijn van drie jaar".

In arrest nr. 73/2020 van 28 mei 2020 heeft het Grondwettelijk Hof het volgende geoordeeld:

"B.4. Het in het geding zijnde verschil in behandeling berust op het criterium van de te volgen strafrechtelijke of administratiefrechtelijke procedure. Wanneer de dader strafrechtelijk

[29] Zie in die zin met name advies 75.019/4 en advies 75.809/4 van 24 april 2024 over een voorontwerp van ordonnantie van het Brussels Hoofdstedelijk Gewest 'tot wijziging van sommige bepalingen van het Brussels Wetboek van Ruimtelijke Ordening'.

[30] Zie EHRM 29 juni 2007, *O'Halloran en Francis v. Verenigd Koninkrijk*. Zie ook EHRM 21 april 2009, *Marttinen v. Finland*. Zie over deze kwestie C. Savonet, "Le droit au silence: un droit relatif?", *Rev. Trim. Dr. Homme*, 2009, 763 e.v. Meer specifiek met betrekking tot het Belgische recht: F. Kefer, "Questions à propos du délit d'obstacle à surveillance en droit belge", *Rev. Trim. Dr. Homme*, 2003, 1305 e.v.

[31] Terwijl de gevangenisstraf voor de oorspronkelijke inbreuk krachtens het eerste lid van dezelfde paragraaf vastgesteld wordt op acht dagen tot een jaar.

le droit de ne pas s'auto-incriminer est garanti par l'article 14, paragraphe 3, g), du Pacte international relatif aux droits civils et politiques et par l'article 6 de la Convention européenne des droits de l'Homme[29].

La Cour européenne des droits de l'Homme admet certes des exceptions à cette interdiction de "coercition directe" exercée sur le droit de ne pas s'auto-incriminer mais lesdites exceptions sont envisagées de manière restrictive[30].

Ainsi, l'article 38, § 2, n'est admissible que dans les hypothèses dans lesquelles l'obligation de communiquer les informations demandées n'est pas susceptible d'entraîner une méconnaissance du droit au silence.

La même observation s'applique pour l'article 39, § 5, qui prévoit des sanctions administratives à caractère pénal en cas de non-respect des obligations relatives à la conduite des inspections et des audits et pour quiconque empêche ou gêne volontairement la réalisation de l'inspection effectuée par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à la suite de cette inspection ou communique délibérément des informations erronées ou incomplètes.

Articles 38 et 40

L'avant-projet contient des dispositions concernant l'augmentation de la sanction en cas de récidive.

Ainsi l'article 38, § 1er, alinéa 2, prévoit que l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans[31]. Un alourdissement de la peine est également prévu en cas de récidive pour l'infraction sanctionnée pénalement à l'article 38, § 2. L'amende administrative est également doublée "en cas de récidive dans un délai de trois ans", en vertu de l'article 40, § 4, alinéa 2.

Dans son arrêt n° 73/2020 du 28 mai 2020, la Cour constitutionnelle a jugé ce qui suit:

"B.4. La différence de traitement en cause repose sur le critère de la procédure administrative ou pénale suivie. Lorsque le contrevenant est sanctionné pénalement, la peine

[29] En ce sens, voir notamment l'avis 75.019/4 et l'avis 75.809/4 donné le 24 avril 2024 sur un avant-projet d'ordonnance de la Région de Bruxelles-Capitale "modifiant certaines dispositions du Code bruxellois de l'aménagement du territoire".

[30] Voir Cour eur. D.H., arrêt *O'Halloran et Francis c. Royaume-Uni*, 29 juin 2007. Voir aussi, Cour eur. D.H., arrêt *Marttinen c. Finlande*, 21 avril 2009. Sur la question, voir C. SAVONET, "Le droit au silence: un droit relatif?", Rev. Trim. Dr. Homme, 2009, pp. 763 et s. Plus spécifiquement en rapport avec le droit belge, voir F. Kefer, "Questions à propos du délit d'obstacle à la surveillance en droit belge", Rev. Trim. Dr. Homme, 2003, pp. 1305 et s.

[31] Tandis que la peine d'emprisonnement pour l'infraction initiale est fixée de huit jours à un an en vertu de l'alinéa 1er du même paragraphe.

wordt bestraft, kan de voor het tweede misdrijf opgelopen straf alleen worden verzwaard indien het eerste misdrijf is bestraft bij een in kracht van gewijsde gegane rechterlijke beslissing. Wanneer hij het voorwerp uitmaakt van een administratieve geldboete, kan het bedrag van die boete worden verhoogd indien al eerder een proces-verbaal te zijnen laste werd opgesteld, zelfs indien die vaststelling niet door een sanctie werd gevolgd of indien de administratieve sanctie het voorwerp uitmaakt van een beroep dat nog steeds hangende is.

B.5. Zonder dat het nodig is te oordelen over de vraag of de in het geding zijnde bepaling moet worden gekwalificeerd als een regel die een 'recidive' vastlegt, volstaat het vast te stellen dat zij in een verhoging voorziet van het bedrag van de opgelopen administratieve geldboete, verhoging die verbonden is aan het gedrag van de dader. Zij vormt bijgevolg een maatregel van individualisering van de administratieve sanctie, die vergelijkbaar is met een verzwaring van de strafrechtelijke sanctie in geval van recidive, zoals geregeld bij artikel 23 van de in het geding zijnde ordonnantie.

B.6.1. Wanneer de dader van eenzelfde feit op een alternatieve wijze kan worden gestraft, dat wil zeggen wanneer hij, voor dezelfde feiten, ofwel naar de correctionele rechtbank kan worden verwezen, ofwel een administratieve geldboete kan opgelegd krijgen waartegen hem een beroep wordt geboden voor een andere rechtbank dan een strafrechtbank, dient er een parallellisme te bestaan tussen de maatregelen tot individualisering van de straf.

B.6.2. De eigen kenmerken van de procedure van de administratieve sanctie staan niet eraan in de weg dat alleen de misdrijven waarvan de vaststelling niet het voorwerp heeft uitgemaakt van een beroep of die, in geval van beroep, zijn bevestigd bij een rechterlijke beslissing, in aanmerking worden genomen als grondslag voor een verhoging van de opgelopen administratieve geldboete wanneer het bestrafte misdrijf een herhaling is van een vroeger soortgelijk gedrag van de dader."[32]

Het Grondwettelijk Hof heeft vastgesteld dat de artikelen 10 en 11 van de Grondwet worden geschonden door de betrokken bepaling inzake de verhoging van een administratieve geldboete, "zo geïnterpreteerd dat zij de toepassing ervan niet onderwerpt aan het bestaan van een definitieve voorafgaande administratieve geldboete, die met andere woorden niet langer het voorwerp uitmaakt van een beroep of daarvoor niet meer vatbaar is."[33]

De voornoemde bepalingen van het voorontwerp met betrekking tot de recidive moeten bijgevolg zo worden geformuleerd dat de verhoging enkel kan worden toegepast in geval van een definitieve beslissing tot schuldigverklaring of tot oplegging van een administratieve geldboete, of in geval van een definitieve gerechtelijke veroordeling tot een gevangenisstraf. De betrokken beslissing mag met andere woorden niet langer het voorwerp uitmaken van een beroep of daarvoor vatbaar zijn.

[32] GwH 28 mei 2020, nr. 73/2020. Zie ook GwH 30 september 2021, nr. 125/2021.

[33] GwH 28 mei 2020, nr. 73/2020, B.8.

encourue pour la seconde infraction ne peut être aggravée que si la première infraction a été sanctionnée par une décision juridictionnelle passée en force de chose jugée. Lorsque le contrevenant se voit infliger une amende administrative, le montant de celle-ci peut être augmenté si un procès-verbal a été antérieurement dressé à sa charge, même si cette constatation n'a pas été suivie de sanction ou si la sanction administrative fait l'objet d'un recours toujours pendant.

B.5. Sans qu'il soit nécessaire de trancher la question de savoir si la disposition en cause doit être qualifiée de règle établissant la 'récidive', il suffit de constater qu'elle prévoit une augmentation du montant de l'amende administrative encourue, liée au comportement du contrevenant. Elle constitue dès lors une mesure d'individualisation de la sanction administrative, semblable à l'aggravation de la sanction pénale en cas de récidive, organisée par l'article 23 de l'ordonnance en cause.

B.6.1. Lorsque l'auteur d'un même fait peut être puni de manière alternative, c'est-à-dire lorsque, pour des mêmes faits, il peut, soit être renvoyé devant le tribunal correctionnel, soit se voir infliger une amende administrative contre laquelle un recours lui est offert devant un tribunal non pénal, un parallélisme doit exister entre les mesures d'individualisation de la peine.

B.6.2. Les caractéristiques spécifiques de la procédure de la sanction administrative ne font pas obstacle à ce que seules les infractions dont la constatation n'a pas fait l'objet d'un recours ou qui, en cas de recours, ont été confirmées par une décision juridictionnelle, soient prises en considération pour fonder une augmentation de l'amende administrative encourue lorsque l'infraction sanctionnée est une réitération d'un comportement similaire passé du contrevenant"[32].

La Cour constitutionnelle a constaté la violation des articles 10 et 11 de la Constitution par la disposition concernée relative à l'augmentation d'une amende administrative, "interprétée comme ne soumettant pas son application à l'existence d'une amende administrative préalable définitive, c'est-à-dire qui ne fait plus l'objet ou n'est plus susceptible d'un recours"[33].

Les dispositions précitées de l'avant-projet relatives à la récidive doivent par conséquent être formulées de manière à ce que l'augmentation ne puisse être appliquée qu'en cas de décision définitive déclarant la culpabilité ou infligeant une amende administrative ou en cas de condamnation judiciaire définitive à un emprisonnement. En d'autres termes, la décision concernée ne peut plus faire l'objet ou être susceptible d'un recours.

[32] C.C., 28 mai 2020, n° 73/2020. Voir également C.C., 30 septembre 2021, n° 125/2021.

[33] C.C., 28 mai 2020, n° 73/2020, B.8.

Artikel 40

Paragraaf 5 bepaalt dat de samenloop van meerdere inbreuken aanleiding kan geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Volgens de rechtspraak van het Grondwettelijk Hof gaat het legaliteitsbeginsel in strafzaken, dat met name voortvloeit uit artikel 7 van het Europees Verdrag voor de rechten van de mens, uit

"van de idee dat de strafwet moet worden geformuleerd in bewoordingen op grond waarvan eenieder, op het ogenblik waarop hij een gedrag aanneemt, kan uitmaken of dat gedrag al dan niet strafbaar is. Het eist dat de wetgever in voldoende nauwkeurige, duidelijke en rechtszekerheid biedende bewoordingen bepaalt welke feiten strafbaar worden gesteld, zodat, enerzijds, diegene die een gedrag aanneemt, vooraf op afdoende wijze kan inschatten wat het strafrechtelijke gevolg van dat gedrag zal zijn en, anderzijds, aan de rechter geen al te grote beoordelingsbevoegdheid wordt gelaten."

Gelet op de hier gememoreerde beginselen, moeten de begrippen "samenloop" en "geheel van de feiten", ingeval meerdere overtredingen worden begaan, worden verduidelijkt zodat hun draagwijdte wordt afgebakend. Zo niet moet de bepaling worden weggelaten.

Artikel 41

Er dient in het tweede lid nader te worden gesteld dat de beoogde termijn van een maand ingaat op de dag van ontvangst van de aangetekende zending die in het eerste lid wordt bedoeld.

Artikel 42

1. Gelet op de strekking van de bepaling dienen in de Franse tekst van paragraaf 1, eerste lid, de woorden "émettre une injonction" te worden vervangen door de woorden "décerner une contrainte", en dient in het vervolg van de bepaling het woord "injonction" te worden vervangen door het woord "contrainte".[34]

2. Op de vraag waarom paragraaf 2 voorziet in een betalingstermijn van vierentwintig uur op straffe van tenuitvoerlegging door beslag, heeft de gemachtigde van de Minister het volgende geantwoord:

"De keuze van vierentwintig uur komt uit de NIS 1 wetgeving. Nu blijkt dat dit aangepast is in de NIS 2-wet naar achtenveertig

[34] Zie bijvoorbeeld artikel 58 van de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid', en artikel 56 van de wet van 26 april 2024 'tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid'.

Article 40

Le paragraphe 5 prévoit que la concomitance de plusieurs infractions peut donner lieu à une seule amende administrative proportionnelle à la gravité de l'infraction dans son ensemble.

Selon la jurisprudence de la Cour constitutionnelle, le principe de légalité en matière pénale qui découle notamment de l'article 7 de la Convention européenne des droits de l'homme,

"procède de l'idée que la loi pénale doit être formulée en des termes qui permettent à chacun de savoir, au moment où il adopte un comportement, si celui-ci est ou non punissable. Il exige que le législateur indique, en des termes suffisamment précis, clairs et offrant la sécurité juridique, quels faits sont sanctionnés, afin, d'une part, que celui qui adopte un comportement puisse évaluer préalablement, de manière satisfaisante, quelle sera la conséquence pénale de ce comportement et afin, d'autre part, que ne soit pas laissé au juge un trop grand pouvoir d'appréciation".

Compte tenu des principes ainsi rappelés, les notions de concomitance et d'"infraction dans son ensemble", alors que plusieurs infractions sont commises, seront précisées afin d'en circonscrire la portée. À défaut, la disposition sera omise.

Article 41

Il convient de préciser, à l'alinéa 2, que le délai d'un mois qui y est prévu commence à courir à dater de la réception de la lettre recommandée visée à l'alinéa 1er.

Article 42

1. Compte tenu de la portée de la disposition, dans la version française, au paragraphe 1er, alinéa 1er, il y a lieu de remplacer les mots "émettre une injonction" par les mots "décerner une contrainte" et, dans la suite de la disposition, de remplacer le mot "injonction" par le mot "contrainte"[34].

2. Interrogé sur la question de savoir pourquoi le paragraphe 2 prévoit un délai de vingt-quatre heures pour payer, sous peine d'exécution par saisie, le délégué de la Ministre a indiqué ce qui suit:

"De keuze van vierentwintig uur komt uit de NIS 1 wetgeving. Nu blijkt dat dit aangepast is in de NIS 2-wet naar achtenveertig

[34] Voir par exemple l'article 58 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et l'article 56 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

uur, dus we stellen voor om dit te wijzigen naar achtenveertig uur zodat de twee wetgevende kaders overeenkomen."

Het dispositief moet in die zin worden aangepast.

Artikel 43

Gelet op de regeling die bij artikel 36 wordt ingevoerd, kan het beoogde geval zich onmogelijk voordoen. Het feit dat een administratieve procedure volbracht is, kan immers niet samen bestaan met strafrechtelijke vervolgingen die hangende zijn of nog moeten komen.

Artikel 44

1. Aan de gemachtigde van de minister is gevraagd:

(i) op welke manier de lijst van opgenomen bepalingen is opgesteld;

(ii) of de artikelen in die lijst thuishoren;

(iii) of de delegatie er inderdaad toe strekt uitsluitend regels te bepalen voor de uitvoering van de verplichtingen, dan wel ook regels om ervan af te wijken;

(iv) of dat artikel voor een correcte omzetting van de richtlijn zorgt;

(v) welke entiteit of persoon wordt bedoeld met de term "de sectoraal bevoegde Minister".

De gemachtigde heeft het volgende geantwoord:

"Met betrekking tot (i) en (ii): deze lijst werd opgesteld op basis van de verplichtingen die rechtstreeks uit de CER-Richtlijn voortkomen. In het voorontwerp van wet wordt in verschillende bepalingen nl. verder gegaan dan wat de CER-Richtlijn oplegt: bijvoorbeeld het aanduiden van kritieke infrastructuur, het uitvoeren van een dreigingsanalyse, etc. Gelet op de bijzondere eigenschappen van de sector Overheid, werd het niet opportuun geacht om alle bijkomende nationale verplichtingen ook van toepassing te maken op deze sector. Daarom werd de lijst in artikel 44 opgesteld, waarin de 'minimale' verplichtingen uit CER, die ten minste van toepassing moeten zijn op deze sector, werden opgesomd.

Met betrekking tot (iii): de delegatie bestaat enkel voor het bepalen van de modaliteiten van de uitvoering van de verplichtingen.

Met betrekking tot (iv): omwille van de bijzondere eigenschappen van de sector overheid en de uitdagingen die deze met zich meebrengen wordt voor deze sector een bijzonder kader opgericht, gebaseerd op de verplichtingen uit de CER-Richtlijn en aangepast aan de specificiteiten van de sector. Voor deze sector zal volledig de ratio legis van de CER-Richtlijn gevolgd worden.

uur, dus we stellen voor om dit te wijzigen naar achtenveertig uur zodat de twee wetgevende kaders overeenkomen".

Le dispositif sera adapté en ce sens

Article 43

Compte tenu du système mis en place par l'article 36, l'hypothèse envisagée ne peut se produire. En effet, le fait qu'une procédure administrative ait été menée à son terme ne peut coexister avec des poursuites pénales qui seraient pendantes ou postérieures.

Article 44

1. Interrogé sur

(i) la manière dont la liste des dispositions reprises a été établie

(ii) l'appartenance des articles à cette liste

(iii) la question de savoir si la délégation consiste bien uniquement à déterminer des modalités d'exécution des obligations ou, également, à y déroger

(iv) la question de savoir si cet article constitue une transposition correcte de la directive

(v) et sur l'entité ou la personne visée par le terme "le Ministre sectoriel compétent",

le délégué de la Ministre a répondu ce qui suit:

"Met betrekking tot (i) en (ii): deze lijst werd opgesteld op basis van de verplichtingen die rechtstreeks uit de CER-Richtlijn voortkomen. In het voorontwerp van wet wordt in verschillende bepalingen nl. verder gegaan dan wat de CER-Richtlijn oplegt: bijvoorbeeld het aanduiden van kritieke infrastructuur, het uitvoeren van een dreigingsanalyse, etc. Gelet op de bijzondere eigenschappen van de sector Overheid, werd het niet opportuun geacht om alle bijkomende nationale verplichtingen ook van toepassing te maken op deze sector. Daarom werd de lijst in artikel 44 opgesteld, waarin de 'minimale' verplichtingen uit CER, die ten minste van toepassing moeten zijn op deze sector, werden opgesomd.

Met betrekking tot (iii): de delegatie bestaat enkel voor het bepalen van de modaliteiten van de uitvoering van de verplichtingen.

Met betrekking tot (iv): omwille van de bijzondere eigenschappen van de sector overheid en de uitdagingen die deze met zich meebrengen wordt voor deze sector een bijzonder kader opgericht, gebaseerd op de verplichtingen uit de CER-Richtlijn en aangepast aan de specificiteiten van de sector. Voor deze sector zal volledig de ratio legis van de CER-Richtlijn gevolgd worden.

Met betrekking tot (v): de verwijzing naar de “sectoraal bevoegde Minister” verwijst naar de bevoegde minister van de aangeduide overheidsdienst. Zoals bepaald in de bijlage, betreft de sector Overheid enkel centrale overheden, en is het dus niet mogelijk dat de kwestie onder de bevoegdheid van de gefedereerde entiteiten valt.”

In verband met de sectoraal bevoegde minister en de omzetting van de CER-richtlijn voor wat de overheden betreft die onder de deelstaten ressorteren, wordt verwezen naar de bijzondere opmerking over de artikelen 3, 11°, en 44, alsook naar de bijlage.

2. Op een vraag over de overeenstemming van artikel 44 met de bespreking ervan, met name wat het begrip “sectoraal bevoegde Minister” betreft, heeft de gemachtigde van de Minister het volgende geantwoord:

“Zoals aangegeven verwijst de memorie van toelichting naar het feit dat een ‘delegatie zal worden gegeven aan de Koning zodat dit sectoraal, en meer bepaald, per bevoegde minister, geregeld kan worden’. Het dispositief van artikel 44 van het voorontwerp van wet bepaalt op zijn beurt het volgende: ‘de Koning bepaalt voor de sector overheid, op voordracht van de sectoraal bevoegde Minister’.

Onzes inziens is het uit de gebruikte bewoording duidelijk dat er een delegatie aan de Koning zal plaatsvinden, meer bepaald de bevoegde minister van de welbepaalde kritieke entiteit.”

Er blijkt niet duidelijk genoeg, in ieder geval niet uit de Franse tekst, of het voorontwerp met betrekking tot de sector overheid één dan wel meerdere bevoegde ministers bedoelt wanneer het bijvoorbeeld gaat om de digitale of elektriciteitsinfrastructuur. Het dispositief en de bespreking moeten nauwkeuriger worden geredigeerd zodat hierover geen onduidelijkheid bestaat.

Artikelen 48 en 49

In tegenstelling tot wat deze artikelen aangeven, strekken ze er niet toe wijzigingen aan te brengen in de – onbestaande – artikelen 4 en 7 van de wet van 14 februari 2023 ‘houdende instemming met het samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaamse Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen’. Ze brengen echter wel wijzigingen aan in de artikelen 4 en 7 van het samenwerkingsakkoord van 30 november 2022.

Met betrekking tot (v): de verwijzing naar de “sectoraal bevoegde Minister” verwijst naar de bevoegde minister van de aangeduide overheidsdienst. Zoals bepaald in de bijlage, betreft de sector Overheid enkel centrale overheden, en is het dus niet mogelijk dat de kwestie onder de bevoegdheid van de gefedereerde entiteiten valt”.

Concernant le ministre sectoriel compétent et la question de la transposition de la directive CER en ce qui concerne les administrations publiques relevant des entités fédérées, il est renvoyé à l’observation particulière formulée à propos des articles 3, 11°, et 44 et de l’annexe.

2. Interrogé sur la correspondance entre l’article 44 et son commentaire, notamment quant à la notion de “ministre sectoriel compétent”, le délégué de la Ministre a répondu ce qui suit:

“Zoals aangegeven verwijst de memorie van toelichting naar het feit dat een ‘delegatie zal worden gegeven aan de Koning zodat dit sectoraal, en meer bepaald, per bevoegde minister, geregeld kan worden’. Het dispositief van artikel 44 van het voorontwerp van wet bepaalt op zijn beurt het volgende: ‘de Koning bepaalt voor de sector overheid, op voordracht van de sectoraal bevoegde Minister’.

Onzes inziens is het uit de gebruikte bewoording duidelijk dat er een delegatie aan de Koning zal plaatsvinden, meer bepaald de bevoegde minister van de welbepaalde kritieke entiteit”.

Il n’apparaît pas suffisamment clairement, en tout cas dans la version française, si l’avant-projet vise un seul ministre compétent pour le secteur des administrations publiques ou plusieurs ministres compétents lorsqu’il s’agit par exemple d’infrastructure numérique ou d’électricité. Le dispositif et son commentaire seront mieux précisés pour éviter toute ambiguïté sur ce point.

Articles 48 et 49

Contrairement à ce qu’ils indiquent, ces articles ne visent pas à apporter des modifications aux articles 4 et 7, inexistants, de la loi du 14 février 2023 ‘portant assentiment de l’accord de coopération du 30 novembre 2022 entre l’État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire commune visant à instaurer un mécanisme de filtrage des investissements directs étrangers’, mais aux articles 4 et 7 de l’accord de coopération du 30 novembre 2022.

Een samenwerkingsakkoord mag echter alleen worden gewijzigd als alle betrokken partijen samen dat wensen, en dus alleen middels een ander samenwerkingsakkoord.[35]

De artikelen 48 en 49 moeten bijgevolg worden weggelaten.

Artikel 51

De steller van het voorontwerp moet punt 3° aanpassen zodat ook de woorden “of in de artikelen 2, eerste lid, 1° en 9°,” worden weggelaten uit artikel 6, § 3, van de wet van 20 juli 2022.

Artikel 52

De steller van het voorontwerp moet de voorliggende bepaling aandachtig herlezen om zich ervan te vergewissen dat alle wijzigingen die moeten worden aangebracht in artikel 16, § 4, van de wet van 20 juli 2022, inderdaad worden aangebracht. De afdeling Wetgeving merkt onder andere op dat punt 4°, zoals het nu is geredigeerd, het opschrift van het koninklijk besluit van 2 december 2011 wijzigt (wat niet de bedoeling lijkt te zijn van de steller van voorontwerp), dat niet alle verwijzingen naar de wet van 1 juli 2011 aangepast zijn, of nog dat de wijziging die in punt 5° wordt beoogd betrekking heeft op het derde lid in plaats van op het tweede lid van artikel 16, § 4.

Artikel 53

1. In punt 5° moeten de woorden “in het tweede lid” worden vervangen door de woorden “in het derde lid”.

2. De steller van het voorontwerp moet bovendien nagaan of artikel 17, § 3, van de wet van 20 juli 2022 niet moet worden aangepast om de verwijzingen naar de wet van 1 juli 2011 te wijzigen.

Artikel 55

1. Het citaat uit artikel 14 van de wet van 17 januari 2003 ‘met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector’ in de Franse tekst van punt 1°, a), is niet correct. Het moet worden verbeterd.

2. In punt 2° dient men te schrijven “de bepaling onder paragraaf 2, 7°, wordt opgeheven”, aangezien er noch een punt 1, noch een eerste lid voorkomt in artikel 14, § 2, van de wet van 17 januari 2003.

[35] Zie onder meer advies 20.419/8 van 6 december 1990 over een voorontwerp van wet “betreffende het Instituut voor Hygiëne en Epidemiologie”.

Or, un accord de coopération ne peut être modifié que par la volonté conjuguée de toutes les parties concernées et donc par un autre accord de coopération[35].

Les articles 48 et 49 seront par conséquent omis.

Article 51

L’auteure de l’avant-projet adaptera le 3° pour supprimer également, à l’article 6, § 3, de la loi du 20 juillet 2022, les mots “ou aux articles 2, alinéa 1er, 1° et 9°,”.

Article 52

L’auteure de l’avant-projet relira minutieusement la disposition examinée pour s’assurer que l’ensemble des modifications à apporter à l’article 16, § 4, de la loi du 20 juillet 2022 sont bien effectuées. La section de législation remarque, entre autres, que le 4°, tel qu’il est rédigé, modifie l’intitulé de l’arrêté royal du 2 décembre 2011, ce qui ne semble pas être la volonté de l’auteure de l’avant-projet, que toutes les références à la loi du 1er juillet 2011 ne sont pas adaptées ou encore que la modification prévue au 5° concerne l’alinéa 3 et non l’alinéa 2 de l’article 16, § 4.

Article 53

1. Au 5°, les mots “dans le deuxième alinéa” seront remplacés par les mots “à l’alinéa 3”.

2. L’auteure de l’avant-projet examinera par ailleurs s’il n’y a pas lieu d’adapter l’article 17, § 3, de la loi du 20 juillet 2022 pour modifier les renvois effectués à la loi du 1er juillet 2011.

Article 55

1. Au 1°, a), dans le texte français, la citation issue de l’article 14 de la loi du 17 janvier 2003 ‘relative au statut du régulateur des secteurs des postes et des télécommunications belges’ est incorrecte et sera corrigée.

2. Au 2°, on écrira “la disposition prévue au paragraphe 2, 7°, est abrogée” étant donné qu’il n’y a ni point 1 ni alinéa 1er à l’article 14, § 2, de la loi du 17 janvier 2003.

[35] Voir notamment l’avis 20.419/8 donné le 6 décembre 1990 sur un avant-projet de loi “relatif à l’Institut d’Hygiène et d’Épidémiologie”.

Artikel 74

Het artikel bepaalt het volgende:

"De Koning neemt, bij een in Ministerraad overlegd besluit, de nodige maatregelen, met inbegrip van de opheffing, de aanvulling, de wijziging of de vervanging van wetsbepalingen, om de omzetting van de Europese richtlijnen betreffende de kritieke entiteiten te verzekeren." En voorts: "Hij kan, bij een in Ministerraad overlegd besluit, de bepalingen van Hoofdstukken 4 tot en met 7 en de uitvoeringsbesluiten ervan volledig of gedeeltelijk van toepassing maken op andere sectoren dan diegene bedoeld in de Bijlage."

Het gaat hier om een erg ruime delegatie, die de uitvoerende macht bovendien de mogelijkheid biedt wettelijke bepalingen te vervangen.

In de bespreking wordt die delegatie als volgt verantwoord:

"Omdat de Richtlijn slechts een minimumharmonisatie voorziet, en dat het daarnaast in de toekomst opportuun kan blijken om nieuwe sectoren aan te duiden of de draagwijdte van bepaalde sectoren uit te breiden, wordt aan de Koning machtiging gegeven om wetsbepalingen op te heffen, aan te vullen, te wijzigen of te vervangen met het oog op het verzekeren van n de omzetting van de Europese richtlijnen met betrekking tot de weerbaarheid van kritieke entiteiten. Gelet op de huidige geopolitieke situatie houdt de weerbaarheid van kritieke entiteiten immers een prioriteit in, zowel op Europees als nationaal niveau. Inderdaad, wanneer een toekomstige richtlijn nieuwe sectoren zal toevoegen, of de bestaande verplichtingen zal aanpassen, zal het gaan om het aanbrengen van technische aanpassingen aan de regelgeving, zonder dat een beweegruimte wordt gelaten aan de lidstaten. Derhalve is het volkomen gerechtvaardigd een machtiging te geven aan de Koning om deze aanpassingen aan te brengen. Daarnaast wordt dezelfde machtiging aan de Koning gegeven om de regels op vlak van de weerbaarheid van kritieke entiteiten uit te breiden naar andere sectoren voor dewelke in de toekomst de bescherming van hun weerbaarheid noodzakelijk zou blijken in het belang van de ene of de andere essentiële dienstverlening."

Op een vraag daarover heeft de gemachtigde van de Minister het volgende geantwoord:

"Het verlenen van dergelijke delegatie aan de Koning beoogt dit ontwerp van wet 'future-proof' te maken. Gelet op het huidige geopolitiek klimaat en steeds veranderend risicolandschap, is het noodzakelijk om, wanneer nodig, de wet te kunnen aanpassen aan eventuele wijzigingen van de Europese Richtlijnen hieromtrent. Het is daarnaast mogelijk dat in de toekomst de noodzaak gezien wordt om de nationale verplichtingen toe te voegen aan de wet of te wijzigen, hetgeen mogelijk is gelet op artikel 3 van de CER richtlijn.

Uiteraard zullen dergelijke wijzigingen enkel kunnen gebeuren indien deze overeenstemmen met de CER Richtlijn."

Article 74

Il est prévu que

"[l]e Roi prend, par arrêté délibéré en Conseil des ministres les mesures nécessaires, y compris l'abrogation, l'ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition des directives européennes concernant les entités critiques' et qu'"Il peut, par arrêté délibéré en Conseil des ministres, rendre applicables en tout ou en partie les dispositions des Chapitres 4 à 7 inclus et les arrêtés d'exécution à d'autres secteurs que ceux visés en Annexe".

Il s'agit là d'une délégation très large et qui permet en outre au pouvoir exécutif de remplacer des dispositions légales.

Le commentaire justifie cette délégation comme suit:

"Étant donné que la Directive prévoit seulement une harmonisation minimale et qu'il peut s'avérer opportun, à l'avenir, de désigner de nouveaux secteurs ou d'étendre la portée de certains secteurs, le Roi est habilité à abroger, ajouter, modifier ou remplacer des dispositions légales en vue d'assurer la transposition des directives européennes en matière de résilience des entités critiques. Vu notamment la situation géopolitique actuelle, la résilience des entités critiques est en effet une priorité, tant au niveau européen que national. En effet, lorsqu'une future directive ajoutera de nouveaux secteurs ou adaptera les obligations existantes, il s'agira d'apporter des adaptations techniques à la réglementation sans laisser de marge de manœuvre aux États membres. Il est par conséquent totalement justifié d'habiliter le Roi à procéder à ces adaptations. En outre, la même habilitation est donnée au Roi pour ce qui est d'étendre les règles de résilience des entités critiques à d'autres secteurs pour lesquels la protection de leur résilience s'avèrerait nécessaire à l'avenir, dans l'intérêt de l'un ou de l'autre service essentiel".

Interrogé sur ce point, le délégué de la Ministre a indiqué ce qui suit:

"Het verlenen van dergelijke delegatie aan de Koning beoogt dit ontwerp van wet 'future-proof' te maken. Gelet op het huidige geopolitiek klimaat en steeds veranderend risicolandschap, is het noodzakelijk om, wanneer nodig, de wet te kunnen aanpassen aan eventuele wijzigingen van de Europese Richtlijnen hieromtrent. Het is daarnaast mogelijk dat in de toekomst de noodzaak gezien wordt om de nationale verplichtingen toe te voegen aan de wet of te wijzigen, hetgeen mogelijk is gelet op artikel 3 van de CER richtlijn.

Uiteraard zullen dergelijke wijzigingen enkel kunnen gebeuren indien deze overeenstemmen met de CER Richtlijn".

Een machtiging die aan de Koning wordt verleend om wetgevende normen te wijzigen, aan te vullen of op te heffen, is in het algemeen toelaatbaar wanneer ze van eerder technische aard is en een kleine beoordelingsmarge laat met betrekking tot de nodige aanpassingen.[36]

Dat is in dezen niet het geval. Omzettingen van Europese richtlijnen brengen immers vaak beleidskeuzes mee die door de wetgevende macht moeten worden gemaakt. Dat geldt des te meer voor een aangelegenheid waarin de Europese wetgever globaal werkt via richtlijnen houdende minimale harmonisering, en waarin de Belgische wetgever zich vervolgens niet beperkt tot het omzetten van die Europese richtlijn, maar ook specifieke nationale maatregelen neemt, zoals *in casu* het geval is.

Bijgevolg moet het deel van de machtiging worden weggelaten dat de Koning toelaat om, bij een besluit vastgesteld na overleg in de Ministerraad, de nodige maatregelen te nemen ter omzetting van de Europese richtlijnen inzake de kritieke entiteiten, met inbegrip van de opheffing, de toevoeging, de wijziging of de vervanging van wettelijke bepalingen.

Artikel 75

De woorden “betreffende de bescherming en beveiliging van kritieke infrastructuren” moeten worden vervangen door de woorden “betreffende de beveiliging en de bescherming van de kritieke infrastructuren”, wat het correcte opschrift is van de wet.

Artikel 78

Luidens de voorliggende bepaling treedt de wet in werking op “de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt”.

Overeenkomstig artikel 4 van de wet van 31 mei 1961 ‘betreffende het gebruik der talen in wetgevingszaken, het opmaken, bekendmaken en inwerkingtreden van wetten en verordeningen’, zijn wetten verbindend in het gehele Rijk de tiende dag na die van hun bekendmaking, tenzij ze een andere termijn bepalen.

Tenzij er een specifieke reden bestaat om af te wijken van de gangbare termijn van inwerkingtreding van wetten, dient te worden afgezien van de onmiddellijke inwerkingtreding, teneinde eenieder een redelijke termijn te geven om kennis te nemen van de nieuwe bepalingen.

[36] *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab “Wetgevingstechniek”, aanbevelingen 7.1.4 en 190 en volgende.

D’une manière générale, une habilitation au Roi permettant de modifier, compléter ou abroger des normes législatives est admissible lorsqu’elle est de nature plutôt technique et qu’une marge de manœuvre peu importante est laissée en ce qui concerne les adaptations qui doivent être apportées[36].

Tel n’est pas le cas en l’occurrence. En effet, les transpositions de directives européennes comprennent souvent des choix politiques, qui doivent être opérés par le pouvoir législatif. Cela est d’autant plus vrai dans une matière dans laquelle le législateur européen opère en général via des directives d’harmonisation minimale et dans le cadre de laquelle le législateur belge ne s’est pas simplement borné à transposer la directive européenne mais a adopté des mesures nationales spécifiques, comme c’est le cas en l’espèce.

La partie de l’habilitation permettant que le Roi prenne, par arrêté délibéré en Conseil des ministres, les mesures nécessaires, y compris l’abrogation, l’ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition des directives européennes concernant les entités critiques sera dès lors omise.

Article 75

Les mots “relative à la protection et à la sécurité des infrastructures critiques” seront remplacés par les mots “relative à la sécurité et à la protection des infrastructures critiques” pour se conformer à l’intitulé correct de la loi.

Article 78

Selon la disposition examinée, la “loi entre en vigueur le jour de sa publication au *Moniteur belge*”.

Conformément à l’article 4 de la loi du 31 mai 1961 ‘relative à l’emploi des langues en matière législative, à la présentation, à la publication et à l’entrée en vigueur des textes légaux et réglementaires’, les lois sont obligatoires dans tout le royaume le dixième jour après celui de leur publication, à moins qu’elles ne fixent un autre délai.

À moins d’une raison spécifique justifiant une dérogation au délai usuel d’entrée en vigueur des lois, il faut renoncer à l’entrée en vigueur immédiate et ce, afin d’accorder à chacun un délai raisonnable pour prendre connaissance des nouvelles dispositions.

[36] *Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires,* www.raadvst-consetat.be*,* recommandations n^{os} 7.1.4 et 190 et suivantes.

Bijlage

1. De bijlage moet worden herzien zodat ze overeenstemt met de bijlage bij de CER-richtlijn. Ze wijkt namelijk op meerdere punten af, zonder dat daar grond voor lijkt te bestaan. Er wordt onder meer op het volgende gewezen. De Franse tekst van de bijlage bij het voorontwerp vermeldt "Exploitants d'installations de production, de stockage et de transport d'hydrogène" terwijl in de bijlage bij de CER-richtlijn sprake is van "Exploitants de systèmes de production, de stockage et de transport d'hydrogène". De Franse tekst van de bijlage bij het voorontwerp vermeldt "Systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil" terwijl in de bijlage bij de CER-richtlijn sprake is van "Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil". De Nederlandse tekst van de bijlage bij het voorontwerp vermeldt "Beheerders van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1 van Richtlijn 2010/40/EU van het Europees Parlement en de Raad" terwijl in de bijlage bij de CER-richtlijn sprake is van "Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad".

2. Aangezien het om een voorontwerp van wetgevende norm gaat, zijn de woorden "Gezien om te worden gevoegd bij het voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten - Vu pour être annexé à l'avant-projet de loi concernant la résilience des entités critiques" overbodig en moeten ze worden weggelaten.[37]

Slotopmerkingen

Het dispositief van het voorontwerp moet in het algemeen grondig worden nagezien op wetgevingstechnisch en taalkundig gebied. Ook de overeenstemming tussen de Nederlandse en de Franse tekst van het ontwerp moet acribisch worden nagegaan. Louter bij wijze van voorbeeld wordt op het volgende gewezen:

1° De woorden "des éléments suivants" in de Franse tekst van artikel 20, § 1, derde lid, worden in de Nederlandse tekst niet weergegeven. Als ze al worden gehandhaafd, moeten ze worden vervangen door de woorden "les éléments suivants";

2° In artikel 22, derde lid, 8°, dient men te schrijven: "2003/361/EG".

3° In de Franse tekst van artikel 52, 2°, moet het woord "lealinéa" worden vervangen door de woorden "l'alinéa 1er".

4° In artikel 71, 1° en 2°, dat strekt tot wijziging van artikel 45, § 1, van de wet van 26 april 2024 'tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid', worden de te vervangen woorden niet correct aangegeven.

[37] *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbeveling 172, e).

Annexe

1. L'annexe devra être revue pour correspondre à l'annexe de la directive CER. Plusieurs différences n'apparaissant pas justifiées existent en effet, comme, notamment, "Exploitants d'installations de production, de stockage et de transport d'hydrogène" dans la version française de l'annexe à l'avant-projet tandis que l'annexe à la directive CER traite d'"Exploitants de systèmes de production, de stockage et de transport d'hydrogène" ou encore de "systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil" dans la version française de l'annexe à l'avant-projet alors que l'annexe de la directive CER mentionne des "Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil". La version néerlandaise de l'annexe traite de "Beheerders van intelligente vervoerssystemen gedefinieerd in artikel 4, punt 1 van Richtlijn 2010/40/EU van het Europees Parlement en de Raad", alors que l'annexe de la directive CER mentionne des "Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad".

2. Dès lors qu'il s'agit d'un avant-projet de norme législative, les mots "Gezien om te worden gevoegd bij het voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten - Vu pour être annexé à l'avant-projet de loi concernant la résilience des entités critiques" sont inutiles et seront omis[37].

Observations finales

De manière générale, il conviendra de réexaminer attentivement le dispositif de l'avant-projet sur le plan de la légistique et de la correction de la langue. La concordance entre les versions néerlandaise et française doit elle aussi être minutieusement vérifiée. À titre purement exemplatif, il convient de relever ce qui suit:

1° à l'article 20, § 1er, alinéa 3, les mots "des éléments suivants", qui ne sont pas présents dans la version néerlandaise, devraient être remplacés, s'ils sont maintenus, par les mots "les éléments suivants";

2° à l'article 22, alinéa 3, 8°, il y a lieu d'écrire "2003/361/CE";

3° dans la version française de l'article 52, 2°, le mot "lealinéa" sera remplacé par les mots "l'alinéa 1er";

4° à l'article 71, 1° et 2°, qui vise à modifier l'article 45, § 1er, de la loi du 26 avril 2024 'établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique', les mots indiqués comme devant être remplacés ne sont pas corrects;

[37] *Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, recommandation n° 172, e).

5° In de Franse tekst van de artikelen 35 en 39, § 1, en van de bespreking van artikel 33, dient men “arrêtés d’exécution” te schrijven in plaats van “décrets d’application”.

6° In de Franse tekst van de bijlage dient men in verband met de “Réseaux de chaleur ou de froid” de woorden “Directive (UE) 2018/200147” te vervangen door “Directive (UE) 2018/2001”.

De steller van het voorontwerp moet ook de bespreking van de artikelen aandachtig herlezen om zich ervan te vergewissen dat dat deze spoort met het dispositief en dat de Nederlandse en Franse tekst in overeenstemming zijn.[38]

De griffier, *De voorzitter,*

Béatrice Drapier Patrick Ronvaux

5° aux articles 35 et 39, § 1er, et dans le commentaire de l’article 33, il convient de mentionner non des “décrets d’application” mais des “arrêtés d’exécution”;

6° à l’annexe, en ce qui concerne les réseaux de chaleur et de froid, il y a lieu d’écrire “Directive (UE) 2018/2001” et non “Directive (UE) 2018/200147”.

L’auteure de l’avant-projet relira également attentivement le commentaire des articles afin d’en assurer la cohérence avec le dispositif et entre les versions française et néerlandaise[38].

Le greffier, *Le président,*

Béatrice Drapier Patrick Ronvaux

[38] Zie onder meer:
— de Franse tekst van de bespreking van artikel 18 waarvan de passage “Délégation est également donnée au Roi (…) entité critique” niet volkomen overeenstemt met de Nederlandse tekst, noch met de inhoud van artikel 18, § 6, derde lid;
– de bespreking van artikel 26, in verband met de overheden die aan de kritieke entiteit informatie mogen doorgeven over de dreiging en de externe beschermingsmaatregelen;
– de bespreking van artikel 27, die niet volkomen overeenstemt met de inhoud van dat artikel en die, zoals de gemachtigde van de Minister heeft geopperd, het relevante wettelijke kader ter zake duidelijker zou mogen aangeven;
– de Franse tekst van de bespreking van artikel 33, waarvan de passage “Celle-ci est précédée d’une mise en demeure motivée adressée à l’entité critique” niet volkomen overeenstemt met de Nederlandse tekst, noch met de inhoud van artikel 33;
– de bespreking van artikel 40, betreffende de termijn waarin wordt voorzien voor het horen van de overtreder of voor de schriftelijke voorbereiding van zijn verdediging.

[38] Voir notamment:
— le commentaire de l’article 18, version française dont le passage “Délégation est également donnée au Roi […] entité critique” ne correspond parfaitement ni à la version néerlandaise de ce passage ni au contenu de l’article 18, § 6, alinéa 3;
– le commentaire de l’article 26, en ce qui concerne les autorités pouvant communiquer des informations relatives à la menace et aux mesures externes de protection à l’entité critique;
– le commentaire de l’article 27, qui ne correspond pas totalement à son contenu et qui, comme l’a suggéré le délégué de la Ministre, pourrait mieux expliciter le cadre légal pertinent en la matière;

– le commentaire de l’article 33, version française, dont le passage “Celle-ci est précédée d’une mise en demeure motivée adressée à l’entité critique” ne correspond parfaitement ni à la version néerlandaise de ce passage ni au contenu de l’article 33;
– le commentaire de l’article 40, en ce qui concerne le délai prévu pour que le contrevenant puisse être entendu ou préparer sa défense par écrit.

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de eerste minister, de minister van Economie en Landbouw, de minister van Volksgezondheid, de minister van Financiën, de minister van Justitie, belast met de Noordzee, de minister van Veiligheid en Binnenlandse Zaken, de minister van Mobiliteit, de minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, de minister van Energie en de minister van Middenstand, Zelfstandigen en Kmo's,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De eerste minister, de minister van Economie en Landbouw, de minister van Volksgezondheid, de minister van Financiën, de minister van Justitie, belast met de Noordzee, de minister van Veiligheid en Binnenlandse Zaken, de minister van Mobiliteit, de minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, de minister van Energie en de minister van Middenstand, Zelfstandigen en Kmo's zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:

HOOFDSTUK 1

Algemene bepalingen

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet voorziet in de omzetting van de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

Sur la proposition du premier ministre, du ministre de l'Économie et de l'Agriculture, du ministre de la Santé publique, du ministre des Finances, de la ministre de la Justice, chargée de la Mer du Nord, du ministre de la Sécurité et de l'Intérieur, du ministre de la Mobilité, de la ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique, du ministre de l'Énergie et de la ministre des Classes moyennes, des Indépendants et des PME,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le premier ministre, le ministre de l'Économie et de l'Agriculture, le ministre de la Santé publique, le ministre des Finances, la ministre de la Justice, chargée de la Mer du Nord, le ministre de la Sécurité et de l'Intérieur, le ministre de la Mobilité, la ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique, le ministre de l'Énergie et la ministre des Classes moyennes, des Indépendants et des PME sont chargés de présenter en notre nom à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Dispositions générales

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi transpose la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre

van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG van de Raad.

HOOFDSTUK 2

Definities

Art. 3

Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° OCAD: Coördinatieorgaan voor de dreigingsanalyse ingesteld door artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

2° sectorale overheid: de bevoegde autoriteit, aangewezen in de bijlage bij deze wet of door de Koning, bij besluit vastgesteld na overleg in de Ministerraad, voor de in dezelfde bijlage vermelde sectoren en deelsectoren;

3° kritieke entiteit: een publieke of particuliere entiteit die overeenkomstig hoofdstuk 4, afdeling 1, is geïdentificeerd als behorende tot een van de categorieën opgesomd in bijlage;

4° weerbaarheid: het vermogen van een kritieke entiteit om een incident te voorkomen, te beperken en te beheersen, en om bescherming te bieden en bestand te zijn tegen, te reageren op of, zich aan te passen aan en te herstellen van een incident;

5° incident: elke gebeurtenis die het verlenen van een essentiële dienst aanzienlijk kan verstoren of verstoort, ook wanneer de gebeurtenis gevolgen heeft voor de nationale systemen die de rechtsstaat waarborgen;

6° kritieke infrastructuur: een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, of een onderdeel van een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, hetgeen noodzakelijk is voor de verlening van een essentiële dienst;

7° essentiële dienst: een dienst die van cruciaal belang is voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu;

8° risico: de mogelijkheid van verlies of verstoring als gevolg van een incident, dat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

2022 sur la résilience des entités critiques et abrogeant la directive 2008/114/CE du Conseil.

CHAPITRE 2

Définitions

Art. 3

Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par:

1° OCAM: Organe de coordination pour l'analyse de la menace institué par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° autorité sectorielle: l'autorité compétente désignée dans l'annexe à la présente loi ou par le Roi, par arrêté délibéré en Conseil des ministres, pour les secteurs et sous-secteurs désignés dans la même annexe;

3° entité critique: une entité publique ou privée qui est identifiée comme appartenant à l'une des catégories énumérées en annexe, conformément au chapitre 4, section 1re;

4° résilience: la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir;

5° incident: un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit;

6° infrastructure critique: un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel;

7° service essentiel: un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement;

8° risque: le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise;

9° risicobeoordeling: het gehele proces ter bepaling van de aard en omvang van een risico door potentiële relevante dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden, in kaart te brengen en te analyseren, en door het verlies of de verstoring van een essentiële dienst die dat incident zou kunnen veroorzaken in te schatten;

10° SICAD: Communicatie- en informatiedienst van het arrondissement, zoals bedoeld in artikel 93, § 2, eerste lid, 3° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

11° overheidsinstantie: een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

1° zij is niet van industriële of commerciële aard;

2° zij oefent niet hoofdzakelijk een activiteit uit die tot een van de andere sectoren of deelsectoren uit de bijlage behoren;

3° zij is geen privaatrechtelijke rechtspersoon;

12° NIS 2-wet: de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

13° EEZ: de Belgisch exclusieve economische zone zoals bepaald en afgebakend bij de wet van 22 april 1999 betreffende de exclusieve economische zone van België in de Noordzee.

HOOFDSTUK 3

Toepassingsgebied

Art. 4

Deze wet is mede van toepassing op de Belgische EEZ.

Art. 5

Deze wet is van toepassing op de sectoren en deelsectoren zoals vermeld in bijlage.

Deze wet is echter niet van toepassing op de nucleaire installaties in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen

9° évaluation des risques: l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident;

10° SICAD: Service d'information et de communication de l'arrondissement, tel que visé par l'article 93, § 2, alinéa 1er, 3° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

11° entité de l'administration publique: une autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur de Conseil d'État qui satisfait aux critères suivants:

1° elle n'a pas de caractère industriel ou commercial;

2° elle n'exerce pas à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs de l'annexe;

3° elle n'est pas une personne morale de droit privé;

12° loi NIS 2: la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

13° ZEE: la zone économique exclusive belge telle que définie et délimitée par la loi du 22 avril 1999 concernant la zone économique exclusive de la Belgique en mer du Nord.

CHAPITRE 3

Champ d'application

Art. 4

Cette loi s'applique également dans la ZEE belge.

Art. 5

Cette loi s'applique à tous les secteurs et sous-secteurs mentionnés dans l'annexe à la présente loi.

Toutefois, cette loi ne s'applique pas aux installations nucléaires au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et

voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

Art. 6

§ 1. De bepalingen van hoofdstuk 4, afdeling 2, hoofdstuk 5 en hoofdstuk 7 van deze wet zijn niet van toepassing op de als kritiek geïdentificeerde entiteiten in de sectoren bankwezen, financiëlemarktinfrastructuur en digitale infrastructuur tenzij de Koning anders bepaalt om tot een hoger weerbaarheidsniveau van die kritieke entiteiten te komen.

§ 2. Wanneer bepalingen van sectorspecifieke rechtshandelingen van de Unie vereisen dat kritieke entiteiten maatregelen dienen te nemen om hun weerbaarheid te vergroten, kan de Koning bepalen dat deze maatregelen als gelijkwaardig worden beschouwd aan de verplichtingen uit hoofde van hoofdstuk 4, afdeling 2, hoofdstuk 5 en hoofdstuk 7 van deze wet. In dat geval zijn deze bepalingen niet van toepassing op deze sectoren of deelsectoren.

Art. 7

Deze wet is voor de overheidssector niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten en de algemene inspectie bedoeld in artikel 2, 2° en 3°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie, de Raad van State en het Grondwettelijk Hof;

relative à l'Agence Fédérale du Contrôle Nucléaire, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité.

Art. 6

§ 1er. Les dispositions du chapitre 4, section 2, du chapitre 5 et du chapitre 7 de la présente loi ne s'appliquent pas aux entités identifiées comme critiques dans les secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques, sauf si le Roi en décide autrement pour atteindre un niveau de résilience plus élevé de ces entités critiques.

§ 2. Lorsque des dispositions d'actes juridiques sectoriels de l'Union exigent que les entités critiques adoptent des mesures pour renforcer leur résilience, le Roi peut déterminer que ces mesures sont considérées comme équivalentes aux obligations prévues au chapitre 4, section 2, au chapitre 5 et au chapitre 7 de la présente loi. Dans ce cas, ces dispositions ne s'appliquent pas à ces secteurs ou sous-secteurs.

Art. 7

Pour le secteur de l'administration publique, cette loi ne s'applique pas:

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au ministère de la Défense visé à l'article 1er de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police et à l'inspection générale visés à l'article 2, 2°, et 3°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, en ce compris le Ministère public, le Conseil d'État et la Cour Constitutionnelle;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° het Nationaal Crisiscentrum, opgericht door het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering;

9° nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van NIS2-wet.

Hoofdstuk 4, afdeling 2, en hoofdstukken 5 en 7 van deze wet zijn in elk geval niet van toepassing op kritieke entiteiten die geïdentificeerd werden op grond van hoofdstuk 4, afdeling 1, van deze wet, die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten, of die uitsluitend diensten verlenen aan de in paragraaf 1 bedoelde overheidsinstanties.

HOOFDSTUK 4

Identificatieprocedure

Afdeling 1

Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructuren

Art. 8

§ 1. De sectorale overheid stelt een lijst op van essentiële diensten van de in bijlage genoemde sectoren en deelsectoren. Tijdens het opstellen van deze lijst houdt de sectorale overheid rekening met de Gelegeerde Verordening (EU) 2023/2450 van de Commissie van 25 juli 2023 tot aanvulling van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad door de vaststelling van een lijst van essentiële diensten.

§ 2. De sectorale overheid voert uiterlijk op 17 januari 2026, een risicobeoordeling uit, gebruikmakend van de lijst bedoeld in paragraaf 1, en vervolgens telkens wanneer dat nodig is en ten minste om de vier jaar, teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuren overeenkomstig deze afdeling te identificeren, en die kritieke entiteiten te assisteren bij het nemen van maatregelen uit hoofde van artikel 19.

6° au Service public fédéral Justice crée par l'arrêté royal du 23 mai 2001 portant création du Service public fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visées au 5°;

7° aux missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° au Centre de crise National, institué par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;

9° à l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS2.

En tout état de cause, le chapitre 4, section 2, et les chapitres 5 et 7 de la présente loi ne s'appliquent pas aux entités critiques identifiées conformément au chapitre 4, section 1re, de la présente loi, qui exercent des activités dans le domaine de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales, ou qui fournissent des services exclusivement aux entités de l'administration publique visées au paragraphe 1er.

CHAPITRE 4

Procédure d'identification

Section 1re

Identification et désignation des entités critiques et des infrastructures critiques

Art. 8

§ 1er. L'autorité sectorielle prépare une liste de services essentiels des secteurs et sous-secteurs énumérés en annexe. Lors de sa préparation, l'autorité sectorielle tient compte du règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels.

§ 2. L'autorité sectorielle procède, à l'aide de la liste visée au paragraphe 1er, à une évaluation des risques au plus tard le 17 janvier 2026, et par la suite chaque fois que cela est nécessaire et au moins tous les quatre ans, en vue d'identifier les entités critiques et leurs infrastructures critiques respectives conformément à la présente section, et afin d'assister ces entités critiques à prendre des mesures en vertu de l'article 19.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

§ 3. In de risicobeoordeling wordt rekening gehouden met relevante natuurlijke en door de mens veroorzaakte risico's, met inbegrip van intersectorale of grensoverschrijdende risico's, ongevallen, natuurrampen, noodsituaties op het gebied van volksgezondheid, hybride dreigingen en andere antagonistische dreigingen, waaronder terroristische misdrijven als bedoeld in Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad.

§ 4. Bij de uitvoering van de risicobeoordeling houdt de sectorale overheid, wanneer relevant voor haar sector of deelsector, ten minste rekening met het volgende:

1° de algemene risicobeoordeling die is uitgevoerd overeenkomstig artikel 6, lid 1, van Besluit 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming;

2° andere relevante risicobeoordelingen, uitgevoerd overeenkomstig de voorschriften van de relevante sectorspecifieke wetgeving van de Europese Unie, met inbegrip van Verordening (EU) 2019/941 van het Europees Parlement en de Raad van 5 juni 2019 betreffende risicoparaatheid in de elektriciteitssector en tot intrekking van Richtlijn 2005/89/EG, Verordening (EU) 2017/1938 van het Europees Parlement en de Raad van 25 oktober 2017 betreffende maatregelen tot veiligstelling van de gasleveringszekerheid en houdende intrekking van Verordening (EU) 994/2010, en de Richtlijnen 2007/60/EG van het Europees Parlement en de Raad van 23 oktober 2007 over beoordeling en beheer van overstromingsrisico's en 2012/18/EU van het Europees Parlement en de Raad van 4 juli 2012 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken, houdende wijziging en vervolgens intrekking van Richtlijn 96/82/EG van de Raad;

3° de relevante risico's die voortvloeien uit de afhankelijkheden tussen de in de bijlage bedoelde sectoren, met inbegrip van de afhankelijkheid van in andere lidstaten en derde landen gevestigde entiteiten en de gevolgen die een significante verstoring in één sector kan hebben voor andere sectoren, met inbegrip van significante risico's voor de burgers en de interne markt;

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées, pour les entités critiques potentielles relevant de leurs compétences pour d'autres aspects.

§ 3. L'évaluation de risques tient compte des risques naturels et d'origine humaine pertinents, en ce compris les risques intersectoriels ou transfrontaliers, les accidents, les catastrophes naturelles, les urgences de santé publique, les menaces hybrides et les autres menaces antagonistes notamment les infractions terroristes visées par la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.

§ 4. Lors de l'évaluation des risques, l'autorité sectorielle prend au moins en compte les éléments suivants, lorsque cela est pertinent pour son secteur ou sous-secteur:

1° l'évaluation des risques effectuée conformément à l'article 6, alinéa 1er, de la décision 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union;

2° d'autres évaluations de risques pertinentes réalisées conformément aux exigences de la législation pertinente de l'Union européenne, en ce compris le règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin relatif à la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE, le règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz et abrogeant le règlement (UE) 994/2010, et les directives 2007/60/CE du Parlement européen et du Conseil du 23 octobre 2007 relative à l'évaluation et la gestion des risques d'inondation et 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, modifiant puis abrogeant la directive 96/82/CE du Conseil;

3° les risques pertinents découlant des dépendances entre les secteurs visés en annexe, y compris les dépendances à l'égard d'entités établies dans d'autres États membres et dans des pays tiers, et l'impact qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris les risques importants pour les citoyens et le marché intérieur;

4° alle informatie over incidenten waarvan overeenkomstig artikel 20, paragraaf 1 is kennisgegeven.

Art. 9

§ 1. Binnen een termijn van negen maanden, te rekenen vanaf de inwerkingtreding van deze wet, voert het OCAD een dreigingsanalyse uit voor de sectoren of deelsectoren vermeld in de bijlage.

Deze dreigingsanalyse blijft gedurende maximaal vier jaar geldig vanaf de datum van voltooiing zoals aangegeven in artikel 78. Deze analyse wordt telkens wanneer nodig en ten minste één keer om de vier jaar vernieuwd.

Elke dreigingsanalyse die binnen vier jaar wordt uitgevoerd op basis van andere wetgeving voor de in bijlage vermelde (deel-)sectoren moet voldoen aan de verplichtingen van dit artikel.

§ 2. De dreigingsanalyse bestaat uit een strategische gemeenschappelijke evaluatie zoals bedoeld in artikel 8, eerste lid, 1°, van de wet van 10 juli 2006 betreffende de dreigingsanalyse.

De dreigingsanalyse heeft betrekking op elk type van dreiging die vallen onder de bevoegdheid van de ondersteunende diensten opgesomd in artikel 2, 2°, van voornoemde wet van 10 juli 2006, die door het OCAD pertinent worden geacht ten aanzien van de sector of deelsector.

§ 3. De autoriteit bedoeld in artikel 21, § 1, de sectorale overheden en de ondersteunende diensten van het OCAD delen aan het OCAD alle informatiegegevens dat zij nodig heeft om de dreigingsanalyse uit te voeren zoals bedoeld in paragraaf 1.

§ 4. Onverminderd artikel 10, § 1, van de voornoemde wet van 10 juli 2006 en artikel 8 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst, wordt deze dreigingsanalyse meegedeeld aan de sectorale overheden zodat zij de conclusies ervan kunnen opnemen in de risicoanalyse die zij krachtens artikel 8 moeten uitvoeren.

Art. 10

§ 1. Teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuren die onder haar bevoegdheid vallen te identificeren, overlegt de sectorale overheid

4° toute information sur les incidents notifiés en vertu de l'article 20, paragraphe 1er.

Art. 9

§ 1er. Dans un délai de neuf mois à compter de l'entrée en vigueur de la présente loi, l'OCAM procède à une analyse de la menace pour les secteurs ou sous-secteurs énumérés en annexe.

Cette analyse de la menace reste valable pour un maximum de quatre ans à compter de sa réalisation, comme prévu à l'article 78. Cette analyse est renouvelée chaque fois que nécessaire et au moins une fois tous les quatre ans.

Toute analyse de la menace réalisée endéans les quatre ans sur base d'une autre législation pour les (sous)-secteurs énumérés en annexe doit être conforme aux obligations du présent article.

§ 2. L'analyse de la menace consiste en une évaluation stratégique commune telle que visée à l'article 8, alinéa 1er, 1°, de la loi du 10 juillet 2006 relative à l'analyse de la menace.

L'analyse de la menace vise tout type de menace qui relève de la compétence des services d'appui, énumérés à l'article 2, 2°, de la loi du 10 juillet 2006 susmentionnée, jugée pertinente par l'OCAM en ce qui concerne le secteur ou le sous-secteur.

§ 3. L'autorité visée à l'article 21, § 1er, les autorités sectorielles et les services d'appui de l'OCAM communiquent à l'OCAM toute information dont il a besoin pour effectuer l'analyse de la menace visée au paragraphe 1er.

§ 4. Sans préjudice de l'article 10, § 1er, de la loi du 10 juillet 2006 susmentionnée et de l'article 8 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, cette analyse de la menace est communiquée aux autorités sectorielles afin de leur permettre d'en intégrer les conclusions dans l'analyse de risques qu'elles sont tenues d'effectuer en vertu de l'article 8.

Art. 10

§ 1er. Afin d'identifier les entités critiques et leurs infrastructures critiques respectives relevant de sa compétence, l'autorité sectorielle consulte au préalable l'autorité visée

vooraf met de autoriteit bedoeld in artikel 21, § 1, en raadpleegt zij de potentiële kritieke entiteiten en desgevallend de vertegenwoordigers van de sector.

De potentiële kritieke entiteiten zijn gehouden tot een degelijke informatie-uitwisseling met de sectorale overheid tijdens het identificatieproces.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

De sectorale overheid past de criteria, zoals bedoeld in artikel 11, § 1, toe teneinde een selectie te maken tussen de entiteiten die in haar sector bestaan en stelt een lijst op van de aldus geïdentificeerde potentiële kritieke entiteiten.

Of een incident een aanzienlijk verstorend effect heeft wordt bepaald in functie van de karakteristieken van de betrokken sector, op basis van de criteria bedoeld in artikel 11, § 2.

§ 2. De potentiële kritieke entiteit bezorgt aan de sectorale overheid binnen zes maanden na de raadpleging zoals bedoeld in de eerste paragraaf, een gemotiveerde lijst op van de bijhorende kritieke infrastructuren die noodzakelijk zijn voor de verlening van essentiële diensten. Deze lijst wordt gevalideerd door de bevoegde sectorale overheid, rekening houdende met de criteria uit artikel 11, § 2.

De sectorale overheid behoudt zich het recht voor om deze lijst te wijzigen, met opgave van motivatie hiervoor.

De kritieke entiteit is ten allen tijde verantwoordelijk voor het actualiseren van deze lijst, en stelt binnen dertig dagen na de wijziging de bevoegde sectorale overheid daarvan op de hoogte, met opgave van motivatie hiervoor. Elke wijziging dient gevalideerd te worden door de sectorale overheid. De sectorale overheid stelt op zijn beurt de autoriteit bedoeld in artikel 21, § 1, in kennis van deze wijziging.

De sectorale overheid waakt over de coherentie in haar sector of deelsector voor wat betreft de identificatie van kritieke infrastructuren.

§ 3. De Koning kan de voorwaarden en modaliteiten bepalen voor de informatie uitwisseling in het kader van de identificatieprocedure.

§ 4. Tijdens het identificatieproces wordt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-Wet, betrokken bij het door de sectorale overheden

à l'article 21, § 1er, les entités critiques potentielles et, le cas échéant, les représentants du secteur.

Les entités critiques potentielles sont tenues à des échanges d'informations appropriés avec l'autorité sectorielle au cours du processus d'identification.

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées pour les entités critiques potentielles relevant, pour d'autres aspects, de leurs compétences.

L'autorité sectorielle applique les critères visés à l'article 11, § 1er, afin d'effectuer une sélection parmi les entités existantes dans son secteur, et établit une liste des entités critiques potentielles ainsi identifiées.

L'importance de l'effet perturbateur d'un incident est déterminée en fonction des caractéristiques du secteur concerné, sur la base des critères visés à l'article 11, § 2.

§ 2. L'entité critique potentielle transmet à l'autorité sectorielle, dans un délai de six mois à compter de la consultation visée au paragraphe premier, une liste motivée des infrastructures critiques qui y sont associées et qui sont nécessaires à la fourniture des services essentiels. Cette liste est validée par l'autorité sectorielle compétente, en tenant compte des critères énoncés à l'article 11, § 2.

L'autorité sectorielle se réserve le droit de modifier cette liste, en motivant sa décision.

L'entité critique est en tout temps responsable de la mise à jour de cette liste et informe l'autorité sectorielle compétente endéans les trente jours de la modification, en motivant sa décision. Toute modification doit être validée par l'autorité sectorielle. L'autorité sectorielle informe son tour cette modification à l'autorité visée à l'article 21, § 1er.

L'autorité sectorielle assure la cohérence dans son secteur ou sous-secteur en ce qui concerne l'identification des infrastructures critiques.

§ 3. Le Roi peut déterminer les conditions et les modalités concernant l'échange d'informations dans le cadre de la procédure d'identification.

§ 4. Lors du processus d'identification l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 est associée aux consultations menées par les autorités

en de autoriteit bedoeld in artikel 21, § 1, gevoerde overleg voor de identificatie van de kritieke entiteiten met betrekking tot de cyberbeveiliging van netwerk- en informatiesystemen.

Art. 11

§ 1. De sectorale overheid houdt bij de identificatie van de kritieke entiteiten rekening met de resultaten van de risicobeoordeling uit hoofde van artikel 8 en de nationale strategie zoals bedoeld in artikel 22, en past alle volgende criteria toe:

1° de entiteit verleent één of meer essentiële diensten;

2° de entiteit is actief en haar kritieke infrastructuur bevindt zich op het Belgisch grondgebied;

3° een incident zou een aanzienlijk verstorend effect hebben op de verlening van deze essentiële diensten of andere essentiële diensten van de sectoren die onder het toepassingsgebied vallen van deze wet, zoals bepaald in de bijlage.

§ 2. De sectorale overheid bepaalt, in overleg met de autoriteit bedoeld in artikel 21, § 1, en in voorkomend geval, na raapleging van de betrokken gefedereerde entiteiten, of een incident een aanzienlijk verstorend effect kan hebben op de verlening van essentiële diensten, rekening houdend met de volgende criteria:

1° het belang van de entiteit om de essentiële dienst op een voldoende niveau te houden, rekening houdend met de beschikbare alternatieven voor het verlenen ervan;

2° het aantal gebruikers dat afhankelijk is van de door de entiteit verleende essentiële dienst;

3° het marktaandeel van de entiteit op de markt voor dergelijke diensten;

4° de mate waarin andere in bijlage genoemde sectoren afhankelijk zijn van die essentiële dienst;

5° de ernst en duur van de gevolgen die incidenten kunnen hebben voor de economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging en volksgezondheid;

6° het geografische gebied dat door een incident kan worden getroffen, met inbegrip van eventuele grensoverschrijdende gevolgen;

7° sectorspecifieke of deelsectorspecifieke eigenschappen.

sectorielles et l'autorité visée à l'article 21, § 1er, pour l'identification des entités critiques en ce qui concerne la cybersécurité des réseaux et des systèmes d'information.

Art. 11

§ 1er. Lors de l'identification des entités critiques, l'autorité sectorielle tient compte des résultats de l'évaluation de risques prévue à l'article 8 et de la stratégie nationale visée à l'article 22, et applique tous les critères suivants:

1° l'entité fournit un ou plusieurs services essentiels;

2° l'entité exerce ses activités sur le territoire belge et son infrastructure critique est située sur ledit territoire;

3° un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels ou d'autres services essentiels des secteurs relevant du champ d'application de la présente loi, tels que définis en annexe.

§ 2. L'autorité sectorielle, en concertation avec l'autorité visée à l'article 21, § 1er, et, le cas échéant, après consultation des entités fédérées concernées, détermine si un incident pourrait avoir un effet perturbateur important sur la fourniture des services essentiels, en tenant compte des critères suivants:

1° l'intérêt de l'entité à maintenir un niveau adéquat de fourniture de service essentiel, en tenant compte des alternatives disponibles pour sa fourniture;

2° le nombre d'utilisateurs tributaires du service essentiel fourni par l'entité;

3° la part de marché de l'entité sur le marché de ces services;

4° la mesure dans laquelle d'autres secteurs énumérés en annexe dépendent de ce service essentiel;

5° la gravité et la durée de l'impact que les incidents peuvent avoir sur les activités économiques et sociales, l'environnement, la sûreté et la sécurité publiques et la santé publique;

6° la zone géographique susceptible d'être affectée par un incident, y compris d'éventuels impacts transfrontaliers;

7° les spécificités sectorielles ou sous-sectorielles.

In het geconsolideerd dossier, zoals bedoeld in artikel 12, § 1, onderbouwt de sectorale overheid deze criteria op kwantitatieve en sectorspecifieke of deelsectorspecifieke wijze, voor zover deze gegevens beschikbaar zijn. De autoriteit bedoeld in artikel 21, § 1, kan hierover gemotiveerd relevante informatie opvragen aan de sectorale overheid.

Art. 12

§ 1. De sectorale overheid stelt een geconsolideerd dossier op, bestaande uit de volgende informatie:

1° een lijst van de geïdentificeerde potentiële kritieke entiteiten;

2° een lijst van de geïdentificeerde potentiële kritieke infrastructuren;

3° de gebruikte criteria zoals bedoeld in artikel 11, § 2;

4° een gemotiveerde verantwoording.

De sectorale overheid zendt het geconsolideerd dossier ter advies over aan de autoriteit bedoeld in artikel 21, § 1, en, in voorkomend geval, ter informatie aan de betrokken gefedereerde entiteiten.

Nadat de sectorale overheid het advies bedoeld in het tweede lid ontvangen heeft, duidt zij de kritieke entiteiten en de respectievelijke kritieke infrastructuren aan.

De sectorale overheid informeert de autoriteit bedoeld in artikel 21, § 1, over elke wijziging in het geconsolideerde dossier. De autoriteit bedoeld in artikel 21, § 1, geeft bij elke substantiële wijziging in het geconsolideerde dossier opnieuw advies over die wijziging.

§ 2. Indien geen kritieke entiteit gelegen op het Belgisch grondgebied geïdentificeerd werd binnen een sector of deelsector, zet de bevoegde sectorale overheid, in een schrijven ter attentie van de autoriteit bedoeld in artikel 21, § 1, de redenen uiteen die geleid hebben tot deze afwezigheid van identificatie.

§ 3. De sectorale overheid duidt uiterlijk op 17 juli 2026 de kritieke entiteiten aan.

De sectorale overheid voert het identificatieproces telkens wanneer nodig en minstens één keer om de vier jaar uit, voor wat betreft de kritieke entiteiten die tot haar sector behoren.

Wanneer na de uitvoering van het identificatieproces blijkt dat een eerder aangeduide kritieke entiteit niet

Dans le dossier consolidé, visé à l'article 12, § 1er, l'autorité sectorielle étaie ces critères de manière quantitative et de manière spécifique au secteur ou sous-secteur, pour autant que ces données soient disponibles. L'autorité visée à l'article 21, § 1er, peut, de manière motivée, demander des informations pertinentes à ce sujet à l'autorité sectorielle.

Art. 12

§ 1er. L'autorité sectorielle prépare un dossier consolidé composé des informations suivantes:

1° une liste des entités critiques potentielles identifiées;

2° une liste des infrastructures critiques potentielles identifiées;

3° les critères utilisés tels que visés à l'article 11, § 2;

4° une justification motivée.

L'autorité sectorielle envoie le dossier consolidé pour avis à l'autorité visée à l'article 21, § 1er, et, le cas échéant, pour information aux entités fédérées concernées.

Après avoir reçu l'avis visé à l'alinéa 2, l'autorité sectorielle désigne les entités critiques et les infrastructures critiques respectives.

L'autorité sectorielle informe l'autorité visée à l'article 21, § 1, de toute modification du dossier consolidé. Chaque fois qu'il y a une modification substantielle, l'autorité visée à l'article 21, § 1er, émet un nouvel avis sur toute modification substantielle du dossier consolidé.

§ 2. Si aucune entité critique située sur le territoire belge n'a été identifiée dans un secteur ou sous-secteur, l'autorité sectorielle compétente expose, dans un écrit à l'attention de l'autorité visée à l'article 21, § 1er, les raisons qui ont conduit à cette absence d'identification.

§ 3. L'autorité sectorielle désigne les entités critiques au plus tard le 17 juillet 2026.

L'autorité sectorielle renouvelle le processus d'identification chaque fois que nécessaire et au moins une fois tous les quatre ans en ce qui concerne les entités critiques appartenant à son secteur.

Si, après la réalisation du processus d'identification, il apparaît qu'une entité critique précédemment désignée

meer voldoet aan de criteria uit artikel 11, en bijgevolg niet meer als kritieke entiteit kan worden aangeduid, stelt de bevoegde sectorale overheid deze entiteit tijdig in kennis dat zij niet meer moeten voldoen aan de verplichtingen uit deze wet.

§ 4. De autoriteit bedoeld in artikel 21, § 1, stelt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2 wet binnen een maand na de aanduiding bedoeld in de eerste paragraaf in kennis van de lijst van de entiteiten die werden aangeduid als kritieke entiteiten.

Daarbij wordt, indien van toepassing, vermeld dat het entiteiten betreft die vallen onder de uitzondering van artikel 6, § 1.

Art. 13

§ 1. Binnen een maand na de in artikel 12 bedoelde aanduiding als kritieke entiteit stelt de sectorale overheid de entiteit in kennis van haar met redenen omklede besluit om haar als kritieke entiteit aan te duiden, samen met haar kritieke infrastructuur.

Deze beslissing bevat alle nodige informatie over de verplichtingen waaraan de kritieke entiteit moet voldoen uit hoofde van hoofdstuk 4, afdeling 2, hoofdstuk 5 en hoofdstuk 7 en over de datum vanaf wanneer die verplichtingen van toepassing zijn.

In voorkomend geval, vermeldt de beslissing dat de kritieke entiteiten onder de uitzondering van artikel 6, § 1, vallen.

De sectorale overheid bezorgt aan de autoriteit bedoeld in artikel 21, § 1, een kopie van deze beslissing met de vermelding van de datum van betekening aan de desbetreffende kritieke entiteit.

§ 2. De autoriteit bedoeld in artikel 21, § 1, brengt op de hoogte van deze aanduiding:

1° de burgemeester van de gemeente op het grondgebied waarvan de kritieke infrastructuur van de kritieke entiteit zich bevindt, met het oog op het nemen van externe beschermingsmaatregelen en externe noodplanning;

2° de gouverneur van de provincie op het grondgebied waarvan de kritieke entiteit of haar kritieke infrastructuur zich bevindt of, wanneer de kritieke entiteit zich op het grondgebied van de Brusselse agglomeratie bevindt, de bevoegde overheid krachtens artikel 48 van de bijzondere wet van 12 januari 1989 met betrekking tot de Brusselse instellingen, met het oog op externe noodplanning.

ne répond plus aux critères énoncés à l'article 11 et ne peut donc plus être désignée comme entité critique, l'autorité sectorielle compétente notifie en temps utile à cette entité qu'elle n'est plus tenue de se conformer aux obligations prévues par la présente loi.

§ 4. L'autorité visée à l'article 21, § 1er, notifie à l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 la liste des entités qui ont été désignées comme entités critiques dans un délai d'un mois à compter de la désignation visée à l'alinéa 1er.

Cette notification comprend, le cas échéant, une déclaration indiquant qu'il s'agit d'entités couvertes par l'exception prévue à l'article 6, § 1er.

Art. 13

§ 1er. Dans un délai d'un mois à compter de la désignation visée à l'article 12, l'autorité sectorielle notifie à l'entité sa décision motivée de la désigner comme entité critique, avec son infrastructure critique.

La décision contient toutes les informations nécessaires sur les obligations à respecter par l'entité critique en vertu du chapitre 4, section 2, du chapitre 5 et du chapitre 7, ainsi que la date à partir de laquelle ces obligations leur sont applicables.

Le cas échéant, la décision indique que les entités critiques relèvent de l'exception prévue à l'article 6, § 1er.

L'autorité sectorielle fournit à l'autorité visée à l'article 21, § 1er, une copie de cette décision avec mention de la date de la notification à l'entité critique concernée.

§ 2. L'autorité visée à l'article 21, § 1er, informe de cette désignation:

1° le bourgmestre de la commune sur le territoire de laquelle se trouvent les infrastructures critiques de l'entité critique, afin de prendre des mesures externes de protection et de planification d'urgence externe;

2° le gouverneur de la province sur le territoire de laquelle l'entité critique ou son infrastructure critique se situe ou, lorsque l'entité critique se situe sur le territoire de l'agglomération bruxelloise, l'autorité compétente en vertu de l'article 48 de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises, en vue de la planification d'urgence externe.

De burgemeester en/ of de gouverneur stelt de autoriteit bedoeld in artikel 21, § 1, in kennis in het geval er externe noodplannen worden opgesteld waarin de informatie die zij hebben verkregen op basis van deze paragraaf, verwerkt werd.

§ 3. De autoriteit bedoeld in artikel 21, § 1, bezorgt na de aanduiding van een kritieke entiteit en zijn respectievelijke kritieke infrastructuur, en daarna minstens jaarlijks, aan de door de Koning aangewezen dienst de gemeente waarin de kritieke infrastructuur zich bevindt of, in voorkomend geval, een lijst van de gemeenten waarin de kritieke infrastructuren zich bevinden voor de toepassing van artikel 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Afdeling 2

Kritieke entiteiten
van bijzonder Europees belang

Art. 14

§ 1. Een entiteit wordt als een kritieke entiteit van bijzonder Europees belang beschouwd wanneer zij overeenkomstig artikel 12 als kritieke entiteit werd aangeduid, essentiële diensten verleent aan of in ten minste zes lidstaten, en op grond van paragraaf 3 in kennis gesteld werd van haar aanduiding als kritieke entiteit van bijzonder Europees belang.

§ 2. Na de kennisgeving van haar aanduiding overeenkomstig artikel 13, § 1, dient de kritieke entiteit de bevoegde sectorale overheid te informeren wanneer zij essentiële diensten verleent aan of in zes of meer lidstaten, welke essentiële diensten zij levert aan of in die lidstaten en aan of in welke lidstaten zij die essentiële diensten verleent.

De sectorale overheid stelt de autoriteit bedoeld in artikel 21, § 1, hiervan onverwijld in kennis, zodat zij de Commissie zonder onnodige vertraging in kennis kan stellen van dergelijke kritieke entiteiten.

§ 3. De bevoegde sectorale overheid stelt, nadat zij hiervan op de hoogte gebracht werd door de autoriteit bedoeld in artikel 21, § 1, de betrokken entiteit er onverwijld van in kennis dat zij als kritieke entiteit van bijzonder Europees belang wordt beschouwd. Vanaf de datum van ontvangst van deze kennisgeving zijn de bijkomende verplichtingen van toepassing op de kritieke entiteit van bijzonder Europees belang.

Le bourgmestre et/ou le gouverneur informent l'autorité visée à l'article 21, § 1er, en cas d'élaboration de plans d'urgence externes intégrant les informations qu'ils ont obtenues sur la base du présent paragraphe.

§ 3. Après la désignation d'une entité critique et de son infrastructure critique respective, et au moins une fois par an par la suite, l'autorité visée à l'article 21, § 1er, communique au service désigné par le Roi, la commune dans laquelle l'infrastructure critique se situe ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées en vue de l'application de l'article 126/3 de la loi du 13 juin 2005 relative aux communications électroniques.

Section 2

Entités critiques
revêtant une importance européenne particulière

Art. 14

§ 1er. Une entité est considérée comme une entité critique revêtant une importance européenne particulière pour autant qu'elle ait été désignée comme une entité critique conformément à l'article 12, qu'elle fournisse des services essentiels à ou dans six états membres ou plus, et que sa désignation en tant qu'entité critique revêtant une importance européenne particulière lui ait été notifiée en vertu du paragraphe 3.

§ 2. Suite à la notification de sa désignation conformément à l'article 13, § 1er, l'entité critique doit informer l'autorité sectorielle compétente lorsqu'elle fournit des services essentiels à ou dans six états membres ou plus, quels sont les services essentiels qu'elle fournit à ou dans ces états membres, et à quels États membres elle fournit ces services essentiels.

L'autorité sectorielle en informe l'autorité visée à l'article 21, § 1er, sans délai, afin qu'elle puisse notifier à la Commission, sans retard injustifié, l'identité de ces entités critiques.

§ 3. L'autorité sectorielle compétente, après avoir été informée par l'autorité visée à l'article 21, § 1er, notifie sans délai à l'entité concernée qu'elle est considérée comme une entité critique revêtant une importance européenne particulière. À compter de la date de réception de cette notification, les obligations supplémentaires s'appliquent à l'entité critique d'importance européenne particulière.

Zij informeert haar ook over de aanvullende verplichtingen die op hen rusten en de datum vanaf wanneer deze verplichtingen van toepassing zijn.

§ 4. De kritieke entiteiten van bijzonder Europees belang verlenen toegang aan de adviesmissie opgericht door de Commissie tot informatie, systemen en faciliteiten die betrekking hebben op de verlening van hun essentiële diensten en die de betrokken adviesmissie nodig heeft om haar taken uit te voeren.

De sectorale overheid en de betrokken kritieke entiteit verstrekken aan de Commissie en aan de lidstaten waaraan of waarin de essentiële dienst wordt verleend informatie over de maatregelen die genomen werden naar aanleiding van de aanduiding als kritieke entiteit van bijzonder Europees Belang.

Art. 15

Wanneer dat passend is, raadpleegt het centraal contactpunt, zoals bedoeld in artikel 21, § 1, met de lidstaten van de Europese Unie over kritieke entiteiten, om te zorgen voor een consistente toepassing van de regelgeving omtrent de weerbaarheid van kritieke entiteiten.

Het centraal contactpunt, zoals bedoeld in artikel 21, § 1, is belast met het voeren van bilateraal en multilateraal overleg met de lidstaten van de Europese Unie inzake kritieke entiteiten:

a) die gebruik maken van een kritieke infrastructuur die fysiek verbonden is met twee of meer lidstaten;

b) die deel uitmaken van bedrijfsstructuren die verbonden zijn met of gekoppeld zijn aan kritieke entiteiten in andere lidstaten;

c) die in een lidstaat als zodanig zijn geïdentificeerd en essentiële diensten verlenen aan of in andere lidstaten.

De in lid 1 bedoelde raadplegingen moeten de weerbaarheid van kritieke entiteiten verhogen en, indien mogelijk, de administratieve lasten voor hen verminderen.

Elle l'informe également des obligations supplémentaires qui lui incombent et de la date à partir de laquelle ces obligations sont applicables.

§ 4. Les entités critiques d'importance européenne particulière donnent accès à la mission de conseil établie par la Commission aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels et nécessaires à l'exécution de la mission de conseil concernée.

L'autorité sectorielle et l'entité critique concernée fournissent à la Commission et aux états membres auxquels ou dans lesquels le service essentiel est fourni des informations sur les mesures prises à la suite de la désignation en tant qu'entité critique revêtant une importance européenne particulière.

Art. 15

Chaque fois que cela est approprié, le point de contact central, visé à l'article 21, § 1er, consulte les États membres de l'Union européenne sur les entités critiques aux fins d'assurer l'application cohérente des règles relatives à la résilience des entités critiques.

Le point de contact central, visé à l'article 21, § 1er, est chargé de mener des discussions bilatérales et multilatérales avec les États membres de l'Union européenne sur des entités critiques:

a) qui ont recours à une infrastructure critique qui est physiquement connectée avec deux États membres ou plus;

b) qui font partie de structures d'entreprise connectées ou liées à des entités critiques dans d'autres États membres;

c) qui sont identifiées comme telles dans un État membre et fournissent des services essentiels à ou dans d'autres États membres.

Les consultations visées au paragraphe 1 visent à renforcer la résilience des entités critiques et, si possible, à réduire la charge administrative pesant sur celles-ci.

HOOFDSTUK 5

Interne weerbaarheidsmaatregelen van de kritieke entiteit

Art. 16

De kritieke entiteit duidt een contactpunt kritieke entiteit aan en maakt de contactgegevens ervan over aan de sectorale overheid binnen een termijn van zes maanden vanaf de betekening van de aanduiding als kritieke entiteit, alsook na elke wijziging van deze gegevens.

Het "contactpunt kritieke entiteit" oefent de functie uit van contactpunt ten aanzien van de sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, de burgermeester, de gouverneur, de politiediensten en elke andere bevoegde overheid of openbare dienst voor elke vraag in verband met de weerbaarheid van de entiteit en zijn infrastructuur.

Indien er reeds een "contactpunt kritieke entiteit" werd aangeduid krachtens nationale of Europese bepalingen, maakt de kritieke entiteit de contactgegevens ervan over aan de sectorale overheid.

Het "contactpunt kritieke entiteit" is te allen tijde beschikbaar.

Art. 17

§ 1. De kritieke entiteit maakt een risicobeoordeling van alle relevante risico's die de levering van haar essentiële diensten kunnen verstoren, binnen negen maanden na ontvangst van de in artikel 13, § 1, bedoelde kennisgeving, en vervolgens telkens wanneer dat nodig is, en ten minste om de vier jaar. Daarbij houdt ze rekening met de risicobeoordeling bedoeld in artikel 8, § 2, de dreigingsanalyse bedoeld in artikel 9 die het OCAD opstelt en andere relevante informatie.

De risicobeoordeling van de kritieke entiteit neemt de in artikel 8, § 3, bedoelde relevante risico's in aanmerking die tot een incident zouden kunnen leiden. De risicobeoordeling houdt rekening met de mate waarin andere in bijlage beschreven sectoren afhankelijk zijn van de door de kritieke entiteit verleende essentiële dienst, en de mate waarin die kritieke entiteit afhankelijk is van essentiële diensten van andere entiteiten in andere sectoren, in voorkomend geval tevens in naburige lidstaten en derde landen.

§ 2. Indien een kritieke entiteit reeds risicobeoordelingen heeft uitgevoerd of documenten heeft opgesteld krachtens andere wettelijke bepalingen die relevant zijn

CHAPITRE 5

Mesures internes de la résilience de l'entité critique

Art. 16

L'entité critique désigne un point de contact de l'entité critique et transfère ses coordonnées à l'autorité sectorielle dans un délai de six mois à compter de la notification de la désignation en tant qu'entité critique, ainsi qu'après chaque modification de ces données.

Le "point de contact de l'entité critique" remplit la fonction de point de contact vis-à-vis de l'autorité sectorielle, de l'autorité visée à l'article 21, § 1er, du bourgmestre, du gouverneur, des forces de police, et de tout autre autorité ou service public compétent, pour toute question liée à la résilience de l'entité et de son infrastructure.

Si un "point de contact de l'entité critique" a déjà été désigné en vertu de dispositions nationales ou européennes, l'entité critique transfère ses coordonnées à l'autorité sectorielle.

Le "point de contact de l'entité critique" est disponible à tout moment.

Art. 17

§ 1er. L'entité critique procède à une évaluation de tous les risques pertinents susceptibles de perturber la fourniture de ses services essentiels, dans les neuf mois suivant la réception de la notification visée à l'article 13, § 1er, et par la suite chaque fois que cela est nécessaire, et au moins tous les quatre ans. Ce faisant, elle tient compte de l'évaluation des risques visée à l'article 8, § 2, de l'analyse de la menace effectuée par l'OCAM et visée à l'article 9 et d'autres informations pertinentes.

L'évaluation des risques de l'entité critique prend en considération les risques pertinents visés à l'article 8, § 3, qui pourraient conduire à un incident. L'évaluation des risques tient compte de la mesure dans laquelle d'autres secteurs décrits en annexe dépendent du service fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités dans d'autres secteurs, y compris, le cas échéant, dans les états membres voisins et les pays tiers.

§ 2. Si une entité critique a déjà effectué des évaluations de risques ou préparé des documents en vertu d'autres dispositions légales pertinentes pour son

voor haar risicobeoordeling, kunnen die beoordelingen en documenten gebruikt worden om aan de voorschriften van dit artikel te voldoen, voor zover deze betrekking hebben op de in artikel 8, § 3, bedoelde risico's.

Desgevallend kan de sectorale overheid verklaren dat bestaande risicobeoordelingen die werden uitgevoerd door een kritieke entiteit, waarin de in de tweede paragraaf bedoelde risico's en de mate van afhankelijkheid aan de orde komen, geheel of ten dele voldoen aan de verplichtingen uit hoofde van dit artikel.

Art. 18

§ 1. De kritieke entiteit werkt een weerbaarheidsplan van de entiteit uit, hierna W.P.E. genoemd, met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke entiteit en de weerbaarheid ervan te waarborgen, door het op punt stellen van interne passende en evenredige technische, veiligheids- en organisatorische maatregelen.

Het W.P.E. bevat weerbaarheidsmaatregelen die toegepast worden in functie van de risico's waaraan de entiteit kan worden blootgesteld, rekening houdend met de mogelijkheid tot wijzigende omstandigheden.

Voor een bepaalde sector, of in voorkomend geval, per deelsector, kan de Koning deze maatregelen specifiëren en opleggen om bepaalde informatie op te nemen in het W.P.E.

§ 2. Het W.P.E. bevat minstens:

1° een opsomming van weerbaarheidsmaatregelen, met inbegrip van maatregelen die nodig zijn om:

a) te voorkomen dat incidenten zich voordoen, rekening houdend met maatregelen ter beperking van het risico op rampen en maatregelen voor aanpassing aan de klimaatverandering;

b) te zorgen voor adequate fysieke bescherming van de gebouwen en kritieke infrastructuur, rekening houdend met het plaatsen van omheiningen, het oprichten van barrières, instrumenten en routines voor bewaking van de omgeving, detectieapparatuur en toegangscontroles;

c) de gevolgen van incidenten te bestrijden, te beperken en ertegen bestand te zijn, door te voorzien in aangepaste materiële en organisatorische noodmaatregelen en naar behoren rekening houdend met de uitvoering van de risico- en crisisbeheersingsprocedures en protocollen

évaluation de risques, ces évaluations et documents peuvent être utilisés pour se conformer aux exigences du présent article, dans la mesure où ils concernent les risques visés à l'article 8, § 3.

Le cas échéant, l'autorité sectorielle peut certifier que les évaluations des risques existantes réalisées par une entité critique, qui porte sur les risques et le degré de dépendance visés au deuxième paragraphe, respecte, en tout ou en partie, les obligations prévues par le présente article.

Art. 18

§ 1er. L'entité critique élabore un plan de résilience de l'entité, ci-après dénommé P.R.E., en vue de prévenir, atténuer et neutraliser les risques d'interruption du fonctionnement ou de destruction de l'entité critique et d'assurer la résilience par la mise en place de mesures techniques, de sécurité et organisationnelles internes appropriées et proportionnées.

Le P.R.E. contient des mesures de résilience appliquées en fonction des risques auxquels l'entité peut être exposée, en tenant compte de la possibilité de changements de circonstances.

Pour un secteur donné, ou, le cas échéant, par sous-secteur, le Roi peut préciser ces mesures et imposer d'inclure certaines informations dans le P.R.E.

§ 2. Le P.R.E. contient au moins:

1° une énumération des mesures de résilience, y compris les mesures nécessaires pour:

a) prévenir les incidents, en tenant compte des mesures de réduction des risques de catastrophes et des mesures d'adaptation au changement climatique;

b) assurer une protection physique adéquate des bâtiments et des infrastructures critiques, en tenant compte de l'installation de clôtures, de barrières, d'outils et de routines de surveillance des environs, d'équipements de détection et de contrôles d'accès;

c) traiter, atténuer et résister aux conséquences des incidents, en prévoyant des mesures d'urgence matérielles et organisationnelles appropriées et en tenant dûment compte de la mise en œuvre des procédures et protocoles de gestion des risques et des crises et

en waarschuwingsroutines, hetgeen de vorm kan aannemen van een intern noodplan;

d) te herstellen van incidenten, rekening houdend met bedrijfscontinuïteitsmaatregelen en de identificatie van alternatieve toeleveringsketens, teneinde de verlening van de essentiële dienst te hervatten;

e) te zorgen voor adequaat beheer van personeelsbeveiliging, rekening houdend met maatregelen zoals het vaststellen van categorieën personeelsleden die kritieke functies vervullen, waarbij ook rekening gehouden wordt met personeel van externe dienstverleners, het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en gevoelige informatie, het instellen van procedures voor veiligheidsverificaties zoals bedoeld in artikel 18 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde diensten het aanwijzen van categorieën van personen die aan een dergelijke veiligheidsverificatie moeten worden onderworpen, en het vaststellen van passende opleidingsvoorschriften en kwalificaties;

f) het relevante personeel bewust te maken van de hierboven vermelde maatregelen, naar behoren rekening houdend met opleidingen, informatiemateriaal en oefeningen;

2° de inventaris en de ligging van de kritieke infrastructuur, zoals bedoeld in artikel 10, § 2;

3° de risicobeoordeling vermeld in artikel 17.

§ 3. Binnen een termijn van uiterlijk tien maanden, te rekenen vanaf de betekening van haar aanduiding van als kritieke entiteit zoals bedoeld in artikel 13, past de entiteit de weerbaarheidsmaatregelen uit het W.P.E. toe.

§ 4. Wanneer kritieke entiteiten uit hoofde van nationale of Europese wetgeving, documenten hebben opgesteld en maatregelen hebben genomen die van belang zijn voor de in paragraaf 2 bedoelde maatregelen, dan kunnen zij deze maatregelen en documenten gebruiken om te voldoen aan de voorschriften van dit artikel.

Desgevallend kan de sectorale overheid verklaren dat bestaande weerbaarheidsbevorderende maatregelen genomen door een kritieke entiteit, waarin de in de eerste paragraaf bedoelde technische, beveiligings- en organisatorische maatregelen op passende en evenredige wijze aan de orde komen, geheel of ten dele voldoen aan de verplichtingen uit hoofde van dit artikel.

des routines d'alerte, ce qui peut prendre la forme d'un plan interne d'urgence;

d) pour se remettre d'un incident, en prenant en compte les mesures de continuité de l'activité et l'identification de chaînes d'approvisionnement alternatives afin de reprendre la fourniture du service essentiel;

e) assurer une gestion adéquate de la sécurité du personnel, en tenant compte de mesures telles que l'identification des catégories de personnel exerçant des fonctions critiques, en tenant également compte du personnel des prestataires de services externes, l'établissement de droits d'accès aux bâtiments, aux infrastructures critiques et aux informations sensibles, l'établissement de procédures d'enquête de sécurité visée à l'article 18 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé et l'identification des catégories de personnes devant faire l'objet d'une telle enquête, ainsi que l'établissement d'exigences appropriées en matière de formation et de qualifications;

f) sensibiliser le personnel concerné aux mesures énumérées ci-dessus, en tenant dûment compte de la formation, du matériel d'information et des exercices;

2° l'inventaire et la localisation des infrastructures critiques visées à l'article 10, § 2;

3° l'évaluation des risques visée à l'article 17.

§ 3. Dans un délai de maximum dix mois à compter de la notification de sa désignation comme entité critique visée à l'article 13, l'entité met en œuvre les mesures de résilience du P.R.E.

§ 4. Lorsque les entités critiques ont préparé des plans et des documents en vertu du droit national ou européen qui sont pertinents pour les mesures visées au paragraphe 2, elles peuvent utiliser ces documents pour se conformer aux exigences du présent article.

Le cas échéant, l'autorité sectorielle peut certifier que des mesures existantes de renforcement de la résilience prise par une entité critique, qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles visés au paragraphe premier respectent, en tout ou en partie, les obligations prévues par le présent article.

§ 5. De kritieke entiteit organiseert oefeningen en actualiseert het W.P.E. in functie van de lessen die getrokken worden uit deze oefeningen.

De Koning bepaalt, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de actualiseringen van het W.P.E.

De Koning bepaalt voor een bepaalde sector of, in voorkomend geval, per deelsector, de nadere regels van de deelneming van de relevante overheidsdiensten aan de oefeningen georganiseerd door de kritieke entiteit.

Art. 19

De bevoegde sectorale overheid kan de procedure van artikel 27 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst opstarten, teneinde de uitoefening van een beroep, functie, opdracht of mandaat of de toegang tot lokalen, gebouwen of terreinen aan een veiligheidsverificatie te onderwerpen.

Art. 20

§ 1. Onverminderd de wettelijke of reglementaire bepalingen die, in een bepaalde sector of deelsector, opleggen bepaalde diensten te informeren, is de kritieke entiteit ertoe gehouden, wanneer zich een gebeurtenis voordoet die van aard is om de verlening van essentiële diensten aanzienlijk te verstoren of kunnen verstoren, zo snel mogelijk en uiterlijk binnen 24 uur, tenzij dit operationeel niet mogelijk is, het SICAD, via een rechtstreeks specifiek voorbehouden communicatiekanaal, de door de bevoegde sectorale overheid aangewezen dienst en de autoriteit bedoeld in artikel 21, § 1, te verwittigen.

Deze melding bevat alle beschikbare informatie die nodig is om te bepalen wat de aard, oorzaak en mogelijke gevolgen van het incident zijn, waaronder alle beschikbare informatie die nodig is om te bepalen of er grensoverschrijdende gevolgen zijn.

In voorkomend geval bezorgt de kritieke entiteit uiterlijk een maand later een gedetailleerd verslag over het incident aan de sectorale overheid en de autoriteit bedoeld in artikel 21, § 1.

Om te bepalen of een verstoring aanzienlijk is, wordt rekening gehouden met de volgende elementen:

1° het aantal getroffen gebruikers en hun aandeel;

§ 5. L'entité critique organise des exercices et met à jour le P.R.E., en fonction des enseignements tirés de ces exercices.

Le Roi détermine, pour un secteur ou sous-secteur donné, la fréquence des exercices et des mises à jour du P.R.E.

Le Roi détermine, pour un secteur donné ou, le cas échéant, par sous-secteur, les modalités de la participation des services publics concernés aux exercices organisés par l'entité critique.

Art. 19

L'autorité sectorielle compétente peut initier la procédure prévue à l'article 27 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé, afin de soumettre l'exercice d'une profession, d'une fonction, d'une mission ou d'un mandat, ou l'accès à des locaux, des bâtiments ou des terrains à une vérification de sécurité.

Art. 20

§ 1er. Sans préjudice des dispositions légales ou réglementaires qui imposent, dans un secteur ou sous-secteur donné, d'informer certains services, l'entité critique est tenue, lorsque survient un événement de nature à perturber ou risquant de perturber de manière importante la fourniture de services essentiels, d'en informer dans les meilleurs délais et au plus tard dans les 24 heures, sauf en cas d'impossibilité opérationnelle, le SICAD, par un canal de communication direct et spécifiquement réservé, le service désigné par l'autorité sectorielle compétente et l'autorité visée à l'article 21, § 1er.

Cette notification contient toutes les informations disponibles nécessaires pour déterminer la nature, la cause et les conséquences éventuelles de l'incident, y compris toutes les informations disponibles nécessaires pour déterminer s'il y a des implications transfrontalières.

Le cas échéant, l'entité critique fournit un rapport détaillé sur l'incident à l'autorité sectorielle et l'autorité visée à l'article 21, § 1er, au plus tard dans un délai d'un mois.

Pour déterminer si une perturbation a un caractère important, il convient de prendre en compte les éléments suivants:

1° le nombre d'utilisateurs concernés et leur proportion;

2° de duur van de gebeurtenis;

3° het getroffen geografisch gebied.

In het geval van grensoverschrijdende gevolgen voor de verlening van essentiële diensten in andere lidstaten, meldt de kritieke entiteit dat aan de autoriteit bedoeld in artikel 21, § 1.

§ 2. Het SICAD verwittigt de autoriteit bedoeld in artikel 21, § 1, van elke gebeurtenis waarvan het kennis heeft en die van aard is de verlening van essentiële diensten van de kritieke entiteit aanzienlijk te verstoren en, in voorkomend geval, de autoriteit bedoeld in artikel 16 van de NIS 2 wet.

§ 3. Indien de gebeurtenis van aard is om de verstoring van de werking of de vernietiging van de betrokken kritieke entiteit als gevolg te hebben, verwittigt het centraal contactpunt de bevoegde sectorale overheid en, in het geval het incident aanzienlijke gevolgen heeft of kan hebben voor kritieke entiteiten en voor de continuïteit van de verlening van essentiële diensten in één of meer lidstaten, het centraal contactpunt van de betrokken lidstaten.

Bij het versturen of ontvangen van informatie krachtens deze paragraaf, behandelt het centraal contactpunt die informatie zodanig dat ze vertrouwelijk kan worden gehouden en de veiligheid en de commerciële belangen van de betrokken entiteit worden beschermd.

§ 4. Zo snel mogelijk na een melding als bedoeld in de eerste paragraaf, verstrekt de bevoegde sectorale overheid, in voorkomend geval, de betrokken kritieke entiteit zo spoedig mogelijk relevante vervolginformatie, waaronder informatie die die kritieke entiteit kan helpen om doeltreffend te reageren op het incident in kwestie.

In voorkomend geval, en wanneer zij van oordeel is dat dit in het algemeen belang is, kan de autoriteit bedoeld in artikel 21, § 1, het publiek hierover informeren.

2° la durée de l'événement;

3° la zone géographique concernée.

En cas d'effets transfrontaliers sur la fourniture de services essentiels dans d'autres États membres, l'entité critique en notifie l'autorité visée à l'article 21, § 1er.

§ 2. Le SICAD notifie à l'autorité visée à l'article 21, § 1er, tout événement dont il a connaissance et qui est de nature à perturber de manière importante la fourniture des services essentiels de l'entité critique et, le cas échéant, l'autorité visée à l'article 16 de la loi NIS 2.

§ 3. Si l'événement est de nature à entraîner l'interruption du fonctionnement ou la destruction de l'entité critique concernée, le point de contact central en informe l'autorité sectorielle compétente et, dans le cas où l'incident a ou peut avoir un impact important sur les entités critiques et sur la continuité de la fourniture des services essentiels dans un ou plusieurs États membres, le point de contact central des états membres concernés.

Le point de contact central, qui envoie et reçoit des informations en vertu du présent paragraphe, traite ces informations de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée.

§ 4. Dès que possible après une notification visée au paragraphe 1er, l'autorité sectorielle compétente fournit, le cas échéant, à l'entité critique concernée des informations de suivi pertinentes, y compris des informations susceptibles d'aider cette entité critique à réagir efficacement à l'incident en question.

Le cas échéant, et lorsqu'elle estime que cela est dans l'intérêt public, l'autorité visée à l'article 21, § 1er, peut informer le public en conséquence.

HOOFDSTUK 6

Rapportage en informatie-uitwisseling

Afdeling 1

De bevoegde autoriteiten

Art. 21

§ 1. De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit bedoeld in het eerste lid is ook het Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de lidstaten van de Europese Unie.

Daartoe vertegenwoordigt het contactpunt België binnen de Groep voor de weerbaarheid van kritieke entiteiten.

§ 2. De autoriteit bedoeld in de eerste paragraaf coördineert en voldoet aan de rapportageverplichtingen die voortvloeien uit hoofde van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad inzake de weerbaarheid van kritieke entiteiten.

De Koning kan de coördinerende rol van de autoriteit als bedoeld in de eerste paragraaf voor wat betreft de weerbaarheid van kritieke entiteiten verder preciseren.

§ 3. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de nadere regels bepaald in artikel 92*ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden aan.

Art. 22

De Koning wijst de autoriteit aan die belast is met het opstellen van een nationale strategie om de weerbaarheid van kritieke entiteiten te verbeteren. Deze strategie wordt uiterlijk op 17 januari 2026, en daarna ten minste om de vier jaar opgesteld.

CHAPITRE 6

Rapports et échange d'informations

Section 1re

Les autorités compétentes

Art. 21

§ 1er. Le Roi désigne l'autorité qui, en tant qu'autorité nationale, est chargée du suivi et de la coordination de la mise en œuvre de la présente loi.

L'autorité visée à l'alinéa 1er est également le Point de Contact Central National pour la résilience des entités critiques, pour l'ensemble des secteurs et sous-secteurs, pour la Belgique dans sa relation avec la Commission européenne et les États membres de l'Union européenne.

À cette fin, le point de contact représente la Belgique au sein du Groupe pour la résilience des entités critiques.

§ 2. L'autorité visée au paragraphe premier coordonne et respecte les obligations d'information découlant de la directive (UE) 2022/2557 du Parlement européen et du Conseil relative à la résilience des entités critiques.

Le Roi peut préciser le rôle de coordination de l'autorité visée au paragraphe 1er en ce qui concerne la résilience des entités critiques.

§ 3. Le Roi désigne, par arrêté délibéré en Conseil des ministres, les autorités sectorielles chargées, pour leur secteur respectif, de veiller à l'exécution des dispositions de la présente loi.

Le Roi peut instituer des autorités sectorielles composées de représentants de l'État fédéral, des Communautés et des Régions, selon les modalités prévues à l'article 92*ter* de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Nonobstant l'alinéa 1er, cette loi désigne elle-même les autorités sectorielles établies et réglementées par la loi.

Art. 22

Le Roi désigne l'autorité chargée d'établir une stratégie nationale visant à améliorer la résilience des entités critiques. Cette stratégie est établie au plus tard le 17 janvier 2026, et au moins tous les quatre ans par la suite.

De autoriteit bedoeld in het eerste lid raadpleegt, in voorkomend geval, de sectorale overheden, de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-wet en de gefedereerde entiteiten.

De strategie bevat, voortbouwend op bestaande nationale en sectorale strategieën, alsook op plannen of soortgelijke documenten, strategische doelstellingen en beleidsmaatregelen die ervoor moeten zorgen dat kritieke entiteiten een hoge weerbaarheid hebben en behouden, en die ten minste op de in de bijlage beschreven sectoren betrekking hebben.

De nationale strategie bevat minstens:

1° strategische doelstellingen en prioriteiten ter vergroting van de algehele weerbaarheid van kritieke entiteiten, met inachtneming van grensoverschrijdende, intersectorale en onderlinge afhankelijkheden;

2° een *governance* kader ter verwezenlijking van de strategische doelstellingen en prioriteiten, met inbegrip van een beschrijving van de taken en verantwoordelijkheden van de verschillende autoriteiten, kritieke entiteiten en andere partijen die bij de uitvoering van de strategie betrokken zijn;

3° een beschrijving van de maatregelen die nodig zijn om de algehele weerbaarheid van kritieke entiteiten te vergroten, inclusief een beschrijving van de nationale risicobeoordeling;

4° een beschrijving van het proces waarmee kritieke entiteiten worden geïdentificeerd;

5° een beschrijving van het proces waarmee kritieke entiteiten worden ondersteund, met inbegrip van maatregelen ter verdieping van de samenwerking tussen de publieke sector enerzijds en de particuliere sector en de publieke en particuliere entiteiten anderzijds;

6° een lijst van de belangrijkste autoriteiten en belanghebbenden, met uitzondering van de kritieke entiteiten, die betrokken zijn bij de uitvoering van de strategie;

7° een beleidskader voor de coördinatie tussen de in deze wet bevoegde autoriteiten en de overeenkomstig de NIS 2 wet aangewezen bevoegde autoriteiten, met het oog op de uitwisseling van informatie over cyberbeveiligingsrisico's, cyberdreigingen en -incidenten en niet-cyber gerelateerde risico's, dreigingen en incidenten en de uitoefening van toezichthoudende taken;

8° een beschrijving van de reeds bestaande maatregelen om de uitvoering van de verplichtingen uit hoofde van hoofdstuk 5 door kleine en middelgrote ondernemingen

L'autorité visée à l'alinéa 1er consulte, le cas échéant, les autorités sectorielles, l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 et les entités fédérées.

La stratégie définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe.

La stratégie nationale comprend au moins:

1° des objectifs et priorités stratégiques visant à renforcer la résilience globale des entités critiques en tenant compte des aspects transfrontaliers, intersectoriels et des interdépendances;

2° un cadre de gouvernance pour atteindre les objectifs et priorités stratégiques, y compris une description des rôles et responsabilités des différentes autorités, entités critiques et autres parties impliquées dans la mise en œuvre de la stratégie;

3° une description des mesures nécessaires pour accroître la résilience globale des entités critiques, y compris une description de l'évaluation nationale des risques;

4° une description du processus d'identification des entités critiques;

5° une description du processus de soutien, y compris les mesures visant à approfondir la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part;

6° une liste des principales autorités et parties concernées, à l'exclusion des entités critiques, qui participent à la mise en œuvre de la stratégie;

7° un cadre politique pour la coordination entre les autorités compétentes en vertu de la présente loi et les autorités compétentes désignées conformément à la loi NIS 2, aux fins de l'échange d'informations sur les risques, les menaces et les incidents liés à la cybersécurité et les risques, menaces et incidents non liés à la cybersécurité et l'exercice des fonctions de surveillance;

8° une description des mesures déjà en place pour faciliter la mise en œuvre des obligations du Chapitre 5 par les petites et moyennes entreprises au sens de

in de zin van de bijlage bij de Commissieaanbeveling 2003/361/EC, die de lidstaten als kritieke entiteiten hebben aangemerkt, te vergemakkelijken.

Afdeling 2

Informatie-uitwisseling

Art. 23

De betrokken autoriteiten beperken de toegang tot de bedrijfsinformatie die zij verkrijgen op grond van deze wet, teneinde de veiligheids- en commerciële belangen van kritieke entiteiten te waarborgen.

Art. 24

In voorkomend geval, en wanneer zij van oordeel is dat dit opportuun is, kan de autoriteit bedoeld in art. 21, § 1, voorzien in de verdere facilitering van het vrijwillig delen van informatie tussen kritieke entiteiten over aangelegenheden die betrekking hebben tot hun weerbaarheid.

Art. 25

De autoriteit bedoeld in artikel 21, § 1, het OCAD en, in voorkomend geval, de autoriteit bedoeld in artikel 16 NIS 2 Wet en de sectorale overheid wisselen vanuit hun eigen bevoegdheden, alle nuttige informatie uit voor het nemen van externe beschermingsmaatregelen voor de kritieke entiteiten.

Art. 26

De kritieke entiteit, het contactpunt kritieke entiteit, de sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, het OCAD, en, in voorkomend geval, de autoriteit bedoeld in artikel 16 NIS 2 wet, werken te allen tijde samen, vanuit hun eigen opdracht en bevoegdheden, door middel van een adequate informatie-uitwisseling betreffende de weerbaarheid van de kritieke entiteiten, teneinde te waken over een overeenstemming tussen de interne weerbaarheidsmaatregelen en de externe beschermingsmaatregelen.

De sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, en de kritieke entiteit kunnen, in voorkomend geval, informatie uitwisselen met de gefedereerde entiteiten, voor de kritieke entiteiten die onder hun bevoegdheden vallen.

l'annexe de la Recommandation 2003/361/CE de la Commission, que les États membres ont identifiées comme des entités critiques**.**

Section 2

Échange d'informations

Art. 23

Les autorités compétentes limitent l'accès aux informations commerciales obtenues en vertu de la présente loi afin de préserver la sécurité et les intérêts commerciaux des entités critiques.

Art. 24

Le cas échéant, et lorsqu'elle le juge approprié, l'autorité visée à l'article 21, § 1er, peut prévoir de faciliter davantage le partage volontaire d'informations entre les entités critiques sur des questions liées à leur résilience.

Art. 25

L'autorité visée à l'article 21, § 1er, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi NIS 2 et l'autorité sectorielle s'échangent, dans le cadre de leurs compétences, toute information utile pour la prise de mesures externes de protection des entités critiques.

Art. 26

L'entité critique, le point de contact de l'entité critique, l'autorité sectorielle, l'autorité visée à l'article 21, § 1er, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi NIS 2 collaborent en tout temps, dans le cadre de leurs mission et compétences, par un échange adéquat d'informations concernant la résilience de l'entité critique, afin de veiller à une concordance entre les mesures internes de résilience et les mesures externes de protection.

L'autorité sectorielle, l'autorité visée à l'article 21, § 1er, et l'entité critique peuvent, le cas échéant, échanger des informations avec les entités fédérées, pour les entités critiques relevant de leur compétence.

Art. 27

De Koning kan, voor een bepaalde sector, of in voorkomend geval, per deelsector, de informatie uit het W.P.E. bepalen die pertinent kan zijn voor het vervullen van de opdrachten van de autoriteit bedoeld in artikel 21, § 1, en van het OCAD op het vlak van de weerbaarheid van kritieke entiteiten, en de nadere regels van de toegang tot die informatie bepalen.

Art. 28

De autoriteit bedoeld in artikel 21, § 1, kan aan de kritieke entiteit informatie over de dreiging en over de externe beschermingsmaatregelen overmaken die de entiteit toelaten zijn weerbaarheidsmaatregelen op gepaste wijze toe te passen en ze in overeenstemming te brengen met de externe beschermingsmaatregelen.

De autoriteit bedoeld in artikel 21, § 1, kan een kopie van deze informatie aan de bevoegde sectorale overheid overzenden.

Art. 29

De sectorale overheid, de autoriteit bedoeld in artikel 21, § 1, het OCAD, de autoriteit bedoeld in artikel 16 NIS 2 wet, alsook de burgemeester en de gouverneur, beperken de toegang tot de informatie bedoeld in hoofdstukken 4 en 5, tot de personen die er kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht in het kader van de weerbaarheid van de kritieke entiteiten, zoals bedoeld in deze wet.

Art. 30

Onverminderd artikel 27 zijn de kritieke entiteit, de gouverneur en de burgemeester gehouden tot het beroepsgeheim voor wat de inhoud van het W.P.E. betreft en mag zij enkel toegang geven tot het W.P.E. aan personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht.

De kritieke entiteit is aan hetzelfde geheim gehouden voor wat betreft alle informatie die haar ter kennis wordt gebracht met toepassing van hoofdstuk 4, en de artikelen 18, § 6, 20, 26 en 28.

Inbreuken op eerste en tweede leden worden bestraft met de straffen voorzien bij artikel 458 van het Strafwetboek.

Art. 27

Le Roi peut déterminer, pour un secteur déterminé ou, le cas échéant, par sous-secteur, les informations du P.R.E. qui peuvent être pertinentes pour l'accomplissement des missions de l'autorité visée à l'article 21, § 1er, et de l'OCAM en matière sur résilience des entités critiques, ainsi que les modalités d'accès à ces informations.

Art. 28

L'autorité visée à l'article 21, § 1er, peut communiquer à l'entité critique des informations relatives à la menace et aux mesures externes de protection qui permettent à l'entité d'appliquer ses mesures de résilience de manière appropriée et de les mettre en concordance avec les mesures externes de protection.

L'autorité visée à l'article 21, § 1er, peut transmettre une copie de ces informations à l'autorité sectorielle compétente.

Art. 29

L'autorité sectorielle, l'autorité visée à l'article 21, § 1er, l'OCAM, l'autorité visée à l'article 16 de la loi NIS 2, ainsi que le bourgmestre et le gouverneur, limitent l'accès aux informations visées aux chapitres 4 et 5, aux personnes ayant besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission, dans le contexte de la résilience des entités critiques, telle que visée dans la présente loi.

Art. 30

Sans préjudice de l'article 27, l'entité critique est tenue au secret professionnel en ce qui concerne le contenu du P.R.E. et ne peut donner accès au P.R.E. qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission.

L'entité critique est tenue au même secret en ce qui concerne toutes les informations portées à sa connaissance en application du chapitre 4, et des articles 18, § 6, 20, 26 et 28.

Les infractions aux alinéas 1er et 2 sont punies des peines prévues à l'article 458 du Code pénal.

Art. 31

De wet van 11 april 1994 betreffende de openbaarheid van bestuur is niet van toepassing op informatie, documenten of gegevens, in welke vorm ook, bedoeld in artikel 29.

Art. 32

De sectorale overheid waakt erover dat minstens één iemand van zijn personeel dat toegang heeft tot informatie inzake de weerbaarheid van kritieke entiteiten, zoals bedoeld in de hoofdstukken 4 en 5, beschikt over een veiligheidsmachtiging van het niveau GEHEIM, als bedoeld in hoofdstuk III van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst. De Koning kan, voor een bepaalde sector of deelsector, nadere regels hieromtrent vastleggen.

De Koning kan, op voordracht van de bevoegde federale minister, de classificatie van een deel of van het geheel van het W.P.E. voorzien. Hij houdt er rekening mee dat de bevoegde personen binnen de kritieke entiteit ten allen tijde toegang hebben tot hun volledige W.P.E.

HOOFDSTUK 7

Controle en sancties

Afdeling 1

Inspecties en audits

Art. 33

De Koning stelt per sector, of, in voorkomend geval, per deelsector, een inspectiedienst aan, belast met de controle op de naleving, door de kritieke entiteiten van die sector of deelsector, van de bepalingen van deze wet en van haar uitvoeringsbesluiten.

De bevoegde inspectiedienst kan, onverminderd de mogelijkheid om sancties op te leggen overeenkomstig de afdelingen 2, 3 en 4, aan de betrokken kritieke entiteit opdragen de nodige en evenredige maatregelen te nemen om een eventueel vastgestelde inbreuk op de verplichtingen uit deze wet binnen een door de inspectiedienst bepaalde redelijke termijn te verhelpen. De betrokken kritieke entiteit verstrekt de nodige informatie over de genomen maatregelen aan de inspectiedienst.

Bij een dergelijke opdracht wordt met name rekening gehouden met de ernst van de inbreuk.

Art. 31

La loi du 11 avril 1994 relative à la publicité de l'administration ne s'applique pas aux informations, documents ou données, sous quelque forme que ce soit, visés à l'article 29.

Art. 32

L'autorité sectorielle veille à ce qu'au moins une personne de son personnel ayant accès aux informations relatives à la résilience des entités critiques, visées aux chapitres 4 et 5, dispose d'une habilitation de sécurité de niveau SECRET, telle que visée au chapitre III de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé. Le Roi peut, pour un secteur ou sous-secteur déterminé, fixer d'autres règles à cet égard.

Le Roi peut, sur proposition du ministre fédéral compétent, prévoir la classification de tout ou partie du P.R.E. Ce faisant, il tient compte du fait que les personnes compétentes au sein de l'entité critique ont à tout moment accès à l'ensemble de leur P.R.E.

CHAPITRE 7

Contrôle et sanctions

Section 1re

Inspections et audits

Art. 33

Le Roi institue un service d'inspection par secteur, ou, le cas échéant, par sous-secteur, chargé du contrôle du respect des dispositions de la présente loi et de ses arrêtés d'exécution par les entités critiques dudit secteur ou sous-secteur.

Sans préjudice de la possibilité d'imposer des sanctions conformément aux sections 2, 3 et 4, le service d'inspection peut enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente loi, dans un délai raisonnable fixé par lesdites services d'inspection. L'entité critique concernée fournit à l'inspection les informations nécessaires sur les mesures prises.

Ces injonctions tiennent compte, notamment, de la gravité de la violation.

Art. 34

§ 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de bevoegde sectorale inspectiedienst bij de uitoefening van hun toezichtsopdracht over de volgende toezichtsbevoegdheden, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken op deze wet:

1° toegang vragen tot alle documenten, waaronder het W.P.E., of informatie die nodig zijn voor de uitoefening van hun toezichtsopdracht en hiervan een kopie verkrijgen;

2° overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor;

3° alle informatie inwinnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen weerbaarheidsmaatregelen;

4° de identiteit opnemen van de personen die zich op de door de entiteit gebruikte plaatsen bevinden en van wie ze het verhoor nodig achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze officiële identificatiedocumenten voorleggen;

5° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle door de entiteit gebruikte plaatsen betreden; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter.

§ 2. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de leden van de bevoegde sectorale inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe zij toegang wensen te hebben;

2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum achtenveertig uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn, wordt het plaatsbezoek geacht te zijn geweigerd.

Art. 34

§ 1er. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection sectoriel compétents disposent, dans l'exercice de leur mission de supervision, des compétences de contrôle suivantes, tant dans le cadre de démarches administratives que dans le cadre de la constatation de violations de la présente loi:

1° demander l'accès à et obtenir une copie de tout document ou toute information nécessaire à l'exercice de leur mission de supervision, y compris le P.R.E.;

2° procéder, sur place ou à distance, à tout examen, contrôle et audition;

3° requérir toutes les informations qu'ils estiment nécessaires à l'évaluation des mesures de résilience par l'entité concernée;

4° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'entité et dont ils estiment l'audition nécessaire pour l'exercice de leur mission. À cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification;

5° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'entité; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction.

§ 2. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du service d'inspection sectoriel compétents adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels ils souhaitent avoir accès;

2° les manquements éventuels qui font l'objet du contrôle;

3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire.

Le juge d'instruction décide dans un délai de quarante-huit heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans le délai prescrit, la visite des lieux est réputée être refusée.

De bevoegde sectorale inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.

§ 3. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij heeft worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De leden van de bevoegde sectorale inspectiedienst delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 4. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de leden van de bevoegde sectorale inspectiedienst ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor dit toezicht.

§ 5. De Koning legt de nadere regels van deze controle vast. Deze nadere regels specifiëren onder andere de opdrachten van de inspectiedienst, de frequentie van de controles, de minimale voorwaarden waaraan de

Le service d'inspection de l'autorité sectorielle compétents peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

§ 3. Au début de toute audition, il est communiqué à la personne interrogée:

1° que ses déclarations peuvent être utilisées comme preuve en justice;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennent lors de l'audition ou lors d'une partie de celle-ci.

À la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées.

Les membres du service d'inspection sectoriel compétents qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 4. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres du service d'inspection veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour ledit contrôle.

§ 5. Le Roi fixe les modalités de ce contrôle. Ces modalités définissent, notamment, les missions du service d'inspection, la fréquence des inspections, les conditions minimales à remplir par les membres de

inspectieleden moeten voldoen en de punten waarop de controle dient te gebeuren, of de rapportering die aan de sectorale overheid moeten worden gedaan.

Art. 35

De Koning legt, voor een bepaalde sector, of in voorkomend geval, per deelsector, nadere regels vast met betrekking tot het opleggen en de uitvoering van audits ten aanzien van kritieke entiteiten

Afdeling 2

Procedure van de sancties

Art. 36

§ 1. Wanneer een of meer inbreuken op de bepalingen van deze wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kan de inspectiedienst de betrokken kritieke entiteit in gebreke stellen om zijn verplichtingen na te komen binnen een door hem vastgestelde termijn.

De termijn wordt bepaald, rekening houdend met de werkingsvoorwaarden van de kritieke entiteit en met de te nemen maatregelen.

§ 2. De inspectiedienst deelt de overtreder vooraf, behoudens naar behoren gemotiveerde uitzonderlijke gevallen, op een met redenen omklede wijze, mee dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt, behoudens tegenbewijs, geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de inspectiedienst.

Art. 37

Als de inspectiedienst vaststelt dat de kritieke entiteit geen gevolg geeft aan de ingebrekestelling binnen de vastgestelde termijn, worden de feiten vastgesteld in een door de inspectiedienst opgesteld proces-verbaal. Een kopie van het proces-verbaal wordt naar de bevoegde sectorale overheid gestuurd.

De inspectiedienst stuurt het origineel van het proces-verbaal van de feiten die tot een strafrechtelijke sanctie kunnen leiden naar de procureur des Konings.

l'inspection et les points à inspecter, ou le rapportage à faire aux autorités sectorielles.

Art. 35

Le Roi fixe, pour un secteur particulier ou, le cas échéant, par sous-secteur, des règles supplémentaires concernant l'imposition et la réalisation d'audits à l'égard d'entités critiques.

Section 2

Procédure de sanctions

Art. 36

§ 1er. Lorsqu'une ou plusieurs manquements aux dispositions de la présente loi, de ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes sont constatées, le service d'inspection peut mettre en demeure l'entité critique concernée de remplir ses obligations dans un délai qu'elle fixe.

Le délai est déterminé en tenant compte des conditions d'exploitation de l'entité critique et des mesures à prendre.

§ 2. Le service d'inspection notifie, sauf exceptions dûment justifiées, préalablement l'auteur de l'infraction de manière motivée, son intention de lui adresser une mise en demeure et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de cette information, de présenter ses moyens de défense par écrit ou de demander à être entendu. Sauf preuve contraire, l'information est réputée avoir été reçue par le contrevenant le sixième jour après son envoi par le service d'inspection.

Art. 37

Si le service d'inspection constate que l'entité critique ne se conforme pas à la mise en demeure dans le délai imparti, les faits sont constatés dans un procès-verbal rédigé par le service d'inspection. Une copie du rapport officiel est envoyée à l'autorité sectorielle compétente.

Le service d'inspection envoie l'original du procès-verbal décrivant les faits susceptibles d'entraîner une sanction pénale au procureur du Roi.

Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.

De processen-verbaal hebben bewijskracht tot het tegendeel bewezen is, voor zover een afschrift ervan ter kennis wordt gebracht van de vermoedelijke dader van de inbreuk en, in voorkomend geval, aan de kritieke entiteit binnen een termijn van tien dagen die aanvangt de dag na de vaststelling van de inbreuk.

Art. 38

Inbreuken op de bepalingen van deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke sancties of administratieve sancties.

Art. 39

De procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging wordt of is ingesteld. De dag van ontvangst wordt geacht de derde dag te zijn die volgt op deze waarop het kopie van het proces-verbaal aan de postdiensten overhandigd werd, tenzij de geadresseerde het tegendeel bewijst.

De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten voor het verstrijken van voorgemelde termijn, behalve wanneer de Procureur des Konings vooraf meedeelt dat hij geen gevolg aan de inbreuk wenst te geven.

Wanneer de Procureur des Konings geen kennis geeft van zijn beslissing binnen de vastgestelde termijn of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.

Art. 40

In afwijking van deze afdeling wordt voor de sector vervoer over water, voor inbreuken op deze wet en haar uitvoeringsbesluiten, een administratieve geldboete worden opgelegd met toepassing boek 4 van het Belgisch scheepvaartwetboek en de wet van 25 december 2016 tot instelling van administratieve geldboetes van toepassing in geval van inbreuken op de scheepvaartwetten. De minimale en maximale bedragen van de administratieve geldboete stemmen overeen met de respectieve minimale en maximale bedragen voorzien in afdeling 4 van deze wet.

En même temps, une copie du procès-verbal est envoyée à l'auteur de l'infraction.

Les procès-verbaux font foi jusqu'à preuve du contraire pour autant qu'une copie en soit transmise à l'auteur présumé de l'infraction et, le cas échéant, à l'entité critique, dans un délai de dix jours prenant cours le lendemain du jour de la constatation de l'infraction.

Art. 38

Les violations aux disposition de cette loi ou de ses arrêtés d'exécution peuvent donner lieu soit à des sanctions pénales soit à des sanctions administratives.

Art. 39

Le procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour informer l'autorité sectorielle que des poursuites pénales seront ou ont été engagées. Le jour de réception est réputé être le troisième jour suivant celui où la copie du procès-verbal a été remise aux services postaux, sauf preuve contraire apportée par le destinataire.

L'autorité sectorielle ne peut entamer la procédure visant à infliger une amende administrative avant l'expiration du délai susmentionné, à moins que le Procureur ne notifie au préalable qu'il ne souhaite pas donner suite à l'infraction.

Si le Procureur du Roi ne notifie pas sa décision dans le délai imparti ou s'il renonce aux poursuites pénales, l'autorité sectorielle peut décider d'engager la procédure administrative.

Art. 40

Par dérogation à la présente section, pour le secteur du transport maritime, en cas d'infraction à la présente loi et à ses arrêtés d'exécution, une amende administrative est imposable en application du livre 4 du Code de la marine marchande et de la loi du 25 décembre 2016 fixant les amendes administratives applicables en cas d'infraction à la législation sur la marine marchande. Les montants minimum et maximum de l'amende administrative correspondent aux montants minimum et maximum respectifs prévus à la section 4 de la présente loi.

Afdeling 3

Strafrechtelijke sancties

Art. 41

§ 1. Wordt gestraft met een gevangenisstraf van acht dagen tot een jaar en met een geldboete van 26 euro tot 10.000 euro of met één van die straffen alleen, de kritieke entiteit die de verplichtingen opgelegd door of krachtens deze wet betreffende de interne weerbaarheidsmaatregelen uit hoofdstuk 5 en de uitwisseling van informatie uit hoofdstuk 6, afdeling 2, niet naleeft.

Indien wordt vastgesteld dat de overtreder reeds een in kracht van gewijsde gegane strafrechtelijke veroordeling heeft gekregen op grond van deze afdeling, wordt de geldboete verdubbeld en wordt de overtreder gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.

§ 2. Wordt gestraft met gevangenisstraf van acht dagen tot een maand en met geldboete van 26 euro tot 10.000 euro of met één van die straffen alleen, eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt.

Indien wordt vastgesteld dat de overtreder reeds een in kracht van gewijsde gegane strafrechtelijke veroordeling heeft gekregen op grond van deze afdeling, wordt de geldboete verdubbeld en de overtreder gestraft met een gevangenisstraf van vijftien dagen tot een jaar.

§ 3. De bepalingen van boek I van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op de vermelde inbreuken.

Afdeling 4

Administratieve sancties

Art. 42

§ 1. Elke inbreuk op deze wet, op de uitvoeringsbesluiten of op de administratieve beslissingen die krachtens deze wet genomen worden, kan aanleiding geven tot een administratieve sanctie.

§ 2. Niet-naleving van de verplichtingen betreffende informatie-uitwisseling opgelegd krachtens artikel 10, § 3, wordt bestraft met een geldboete van 500 tot 75.000 euro.

Section 3

Sanctions pénales

Art. 41

§ 1er. Est punie d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 10.000 euros, ou de l'une de ces peines seulement, l'entité critique qui ne respecte pas les obligations imposées par ou en vertu de la présente loi, relatives aux mesures internes de résilience prévues au chapitre 5 et à l'échange d'informations prévu au chapitre 6, section 2.

S'il est établi que l'auteur de l'infraction a déjà fait l'objet d'une décision pénale passée en force de chose jugée en vertu de la présente section, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans.

§ 2. Est puni d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 euros à 10.000 euros, ou de l'une de ces peines seulement, quiconque empêche ou entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou communique sciemment des informations inexactes ou incomplètes.

S'il est établi que l'auteur de l'infraction a déjà fait l'objet d'une décision pénale passée en force de chose jugée en vertu de la présente section, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à un an.

§ 3. Les dispositions du livre 1er du Code pénal, en ce compris le chapitre VII et l'article 85, sont applicables aux dites infractions.

Section 4

Sanctions administratives

Art. 42

§ 1er. Toute violation de la présente loi, des arrêtés d'exécution ou des décisions administratives prises en vertu de la présente loi peut donner lieu à une sanction administrative.

§ 2. Le non-respect des obligations relatives à l'échange d'informations imposées en vertu de l'article 10, § 3, est puni d'une amende allant de 500 à 75.000 euros.

§ 3. Niet-naleving van de verplichtingen betreffende de weerbaarheidsmaatregelen opgelegd door of krachtens hoofdstuk 5 van deze wet, wordt bestraft met een geldboete van 500 tot 100.000 euro.

§ 4. Niet-naleving van de verplichtingen betreffende de uitwisseling van informatie uit hoofdstuk 6, afdeling 2, worden bestraft met een geldboete van 500 tot 100.000 euro.

§ 5. Niet-naleving van de verplichtingen betreffende de uitvoering van inspecties en audits opgelegd krachtens hoofdstuk 7 van deze wet, wordt bestraft met een geldboete van 500 tot 125.000 euro.

Eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, die informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt bestraft met een geldboete van 500 tot 125.000 euro.

Art. 43

§ 1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt, behoudens tegenbewijs, geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de sectorale overheid.

§ 3. Gelet op de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen dezelfde termijn, kan de sectorale overheid een in artikel 42 bedoelde administratieve sanctie opleggen.

§ 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.

Indien binnen drie jaar na het opleggen van een definitieve administratieve sanctie op grond van deze afdeling een nieuwe inbreuk als bedoeld in artikel 42 wordt vastgesteld, wordt de administratieve geldboete verdubbeld.

§ 3. Le non-respect des obligations relatives aux mesures de résilience imposées par ou en vertu du chapitre 5 est puni d'une amende de 500 à 100.000 euros.

§ 4. Le non-respect des obligations relatives à l'échange d'informations prévues au chapitre 6, section 2, est puni d'une amende de 500 à 100.000 euros.

§ 5. Le non-respect des obligations relatives à la conduite des inspections et des audits imposées en vertu du chapitre 7 de la présente loi est puni d'une amende de 500 à 125.000 euros.

Quiconque empêche ou gêne volontairement la réalisation de l'inspection effectuée par les membres du service d'inspection, qui refuse de communiquer les informations qui lui sont demandées à la suite de cette inspection, ou qui communique délibérément des informations erronées ou incomplètes, est puni d'une amende de 500 à 125.000 euros.

Art. 43

§ 1er. La décision d'infliger une amende administrative est motivée. Elle indique également le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité sectorielle communique au préalable au contrevenant sa proposition motivée de sanction administrative et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de la proposition, de présenter ses moyens de défense par écrit ou de demander à être entendu. Sauf preuve contraire, la proposition est réputée avoir été reçue par le contrevenant le sixième jour suivant son envoi par l'autorité sectorielle.

§ 3. Au vu des moyens de défense soulevés dans le délai visé au paragraphe 2 ou en l'absence de réponse du contrevenant dans le même délai, l'autorité sectorielle peut imposer une sanction administrative visée à l'article 42.

§ 4. L'amende administrative est proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de l'infraction.

Si, dans les trois ans suivant l'infliction d'une sanction administrative définitive en vertu de la présente section, un nouveau cas d'infraction visé à l'article 42 est constaté, l'amende administrative est doublée.

§ 5. De sectorale overheid mag besluiten dat de beslissing tot oplegging van een administratieve geldboete niet of slechts gedeeltelijk zal worden ten uitvoer gelegd, voor zover de overtreder geen administratieve sanctie uit afdeling 4 werd opgelegd of niet veroordeeld werd tot een strafsanctie uit afdeling 3 tijdens de vijf jaren die de nieuwe inbreuk voorafgaan.

De sectorale overheid verleent het uitstel bij dezelfde beslissing als die met welke zij de geldboete oplegt. De beslissing waarbij het uitstel wordt toegestaan of geweigerd, moet met redenen omkleed worden.

De proeftermijn mag niet minder zijn dan één jaar en niet meer dan drie jaar, te rekenen van de datum van de kennisgeving van de beslissing tot oplegging van de administratieve geldboete of van het vonnis of het arrest dat in kracht van gewijsde is gegaan.

Het uitstel wordt van rechtswege herroepen ingeval gedurende de proeftijd een nieuwe inbreuk begaan is die de toepassing meebrengt van een strafsanctie uit afdeling 3 of een administratieve geldboete uit afdeling 4.

Het uitstel wordt herroepen bij dezelfde beslissing als die waarbij de strafsanctie of de administratieve geldboete wordt opgelegd voor de nieuwe inbreuk die begaan is tijdens de proefperiode.

De administratieve geldboete die uitvoerbaar wordt als gevolg van de herroeping van het uitstel wordt onbeperkt gecumuleerd met die welke opgelegd is wegens de nieuwe inbreuk.

Art. 44

De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.

Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd. De termijn gaat in op de datum van ontvangst van de in lid 1 bedoelde aangetekende zending.

Art. 45

§ 1. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.

§ 5. L'autorité sectorielle peut décider que la décision d'infliger une amende administrative ne sera pas exécutée, ou ne le sera que partiellement, dans la mesure où l'auteur ne s'est pas vu infliger une sanction administrative en vertu de la section 4 ou n'a pas été condamné à une sanction pénale en vertu de la section 3 au cours des cinq années qui précèdent la nouvelle infraction.

L'autorité sectorielle accorde le sursis par la même décision que celle par laquelle elle inflige l'amende. La décision accordant ou refusant le sursis doit être motivée.

Le délai d'épreuve ne peut être inférieur à un an ni supérieur trois ans, à compter de la date de la notification de la décision infligeant la sanction administrative ou à dater du jugement ou de l'arrêt coulé en force de chose jugée.

Le sursis est révoqué de plein droit en cas de nouvelle infraction commise pendant le délai d'épreuve et ayant entraîné l'application d'une sanction pénale en vertu de la section 3 ou d'une sanction administrative en vertu de la section 4.

Le sursis est révoqué par la même décision que celle par laquelle est infligée la sanction pénale ou la sanction administrative pour la nouvelle infraction commise dans le délai d'épreuve.

La sanction administrative qui devient exécutoire par suite de la révocation du sursis est cumulée sans limite avec celle infligée du chef de la nouvelle infraction.

Art. 44

La décision est notifiée au contrevenant par lettre recommandée.

Une demande de paiement de l'amende dans un délai d'un mois est jointe à la décision. Le délai d'un mois commence à courir à dater de la réception de la lettre recommandée visée à l'alinéa 1er.

Art. 45

§ 1er. Si le contrevenant ne paie pas l'amende administrative dans le délai imparti, la décision d'imposer une amende administrative est exécutoire et l'autorité sectorielle peut décerner une contrainte.

Het dwangbevel wordt uitgevaardigd door de sectorale overheid en ondertekend door haar wettelijke vertegenwoordiger of door een daartoe gemachtigd personeelslid.

Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen achtenveertig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 2. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het verzet wordt ingesteld bij deurwaardersexploot dat wordt betekend aan de sectorale overheid en geregistreerd ter griffie van de rechtbank binnen vijftien dagen na betekening van de dagvaarding tot betaling.

De bepalingen van Hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

Verzet tegen een dwangbevel schorst de tenuitvoerlegging van het dwangbevel en de verjaringstermijn voor de vorderingen waarop het dwangbevel betrekking heeft, totdat er een uitspraak is gedaan over de grond van de zaak. De gevolgen van reeds gelegde bewarende beslagen blijven onbeperkt van kracht.

De sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 3. De kosten van de betekening van het dwangbevel alsmede de kosten van bewarende maatregelen en tenuitvoerlegging komen ten laste van de overtreder wiens verzet niet-ontvankelijk of geheel of gedeeltelijk ongegrond is verklaard.

Deze kosten worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

La contrainte est délivrée par l'autorité sectorielle et signée par son représentant légal ou l'agent habilité par ce dernier.

La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un ordre de payer dans les quarante-huit heures sous peine d'exécution par saisie, ainsi qu'un relevé des sommes réclamées et une copie de la déclaration constatant la force exécutoire.

§ 2. L'auteur de l'infraction peut faire opposition à la contrainte auprès du juge des saisies.

Sous peine de nullité, l'opposition est motivée. L'opposition est introduite par exploit d'huissier signifié à l'autorité sectorielle et enrôlé au greffe dans les quinze jours à compter de la signification de la contrainte payer.

Les dispositions du Chapitre VIII de la première partie du Code judiciaire s'appliquent à ce délai, y compris les prolongations prévues à l'article 50, alinéa 2, et à l'article 55 de ce Code.

L'opposition à la contrainte suspend l'exécution de la contrainte, ainsi que la prescription des créances visées par la contrainte, jusqu'à ce qu'il soit statue sur son fondement. Les effets des saisies conservatoires déjà pratiquées sont maintenus sans limite de temps.

L'autorité sectorielle peut ordonner des saisies conservatoires et exécuter la contrainte en utilisant les moyens d'exécution prévus dans la cinquième partie du Code Judiciaire.

Les paiements partiels effectués à la suite de la signification d'une contrainte ne font pas obstacle à la poursuite de l'action administrative.

§ 3. Les frais de signification de la contrainte ainsi que les frais de mesures conservatoires et d'exécution sont à charge du contrevenant dont l'opposition est déclarée irrecevable ou en tout ou partie non fondée.

Ces frais sont déterminés selon les règles applicables aux actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 46

De sectorale overheid kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

HOOFDSTUK 8

Sector overheid

Art. 47

§ 1. De Koning bepaalt voor de sector overheid, op voordracht van de sectoraal bevoegde minister, de wijze van uitvoering van de verplichtingen uit tenminste onderstaande bepalingen uit deze wet:

— artikel 8;

— artikel 10, § 1 en § 4;

— artikel 11;

— artikel 12, § 3;

— artikel 13;

— artikel 14;

— artikel 16;

— artikel 17;

— artikel 18, §§ 1 tot 5;

— artikel 19;

— artikel 20;

— artikel 33;

— artikel 34;

— artikel 35.

§ 2. De administratieve sancties bedoeld in de artikelen 42 tot en met 46 zijn niet van toepassing op entiteiten die deel uitmaken van de overheidssector.

Art. 46

L'autorité sectorielle ne peut imposer une amende administrative après l'expiration d'une période de trois ans à compter du jour où l'infraction a été commise.

CHAPITRE 8

Secteur des administrations publiques

Art. 47

§ 1. Le Roi détermine pour le secteur des administrations publiques, sur proposition du ministre sectoriel compétent, les modalités d'exécution des obligations découlant au moins des dispositions suivantes de la présente loi:

— article 8;

— article 10, § 1er et § 4;

— article 11;

— article 12, § 3;

— article 13;

— article 14;

— article 16;

— article 17;

— article 18, §§ 1 à 5;

— article 19;

— article 20;

— article 33;

— article 34;

— article 35.

§ 2. Les sanctions administratives visées aux articles 42 à 46 ne s'appliquent pas aux entités faisant partie du secteur de l'administration publique.

HOOFDSTUK 9

Diverse bepalingen

Afdeling 1

Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 48

In artikel 28/3, § 2, eerste lid, 4°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, ingevoegd bij wet van 21 december 2021, worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren” vervangen door de woorden “de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

Art. 49

In artikel 105, § 2, 2°, van dezelfde wet, ingevoegd bij wet van 17 februari 2022, worden de woorden “exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “kritieke entiteit in de zin van de wet ... betreffende de weerbaarheid van kritieke entiteiten.

Art. 50

In artikel 126/3, § 3, j), van dezelfde wet, ingevoegd bij wet van 20 juli 2022, worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 2

Wijziging van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

Art. 51

In artikel 3, § 3, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit worden de woorden “in artikel 6, 2°, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging

CHAPITRE 9

Dispositions diverses

Section 1re

Modification de la loi du 13 juin 2005 relative aux communications électroniques

Art. 48

Dans l’article 28/3, § 2, alinéa 1er, 4°, de la loi du 13 juin 2005 relative aux communications électroniques, inséré par la loi du 21 décembre 2021, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du ... relative à la résilience des entités critiques”;

Art. 49

À l’article 105, § 2, 2°, de la même loi, inséré par la loi du 17 février 2022, les mots “exploitant d’une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “entité critique au sens de la loi ... relative à la résilience des entités critiques.

Art. 50

À l’article 126/3, § 3, j), de la même loi, insérée par la loi du 20 juillet 2022, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du ... relative à la résilience des entités critiques.

Section 2

Modification de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l’information et des communications et portant désignation d’une autorité nationale de certification de cybersécurité

Art. 51

Dans l’article 3, § 3, de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l’information et des communications et portant désignation d’une autorité nationale de certification de cybersécurité, les mots “l’article 6, 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux

van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, in artikel 3, 3°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 2, eerste lid, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" vervangen door de woorden "in artikel 3, 2°, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten".

Art. 52

In artikel 6 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de paragrafen 2 en 3 worden de woorden "de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "de artikelen 3, 2°, en 33, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten";

2° in dezelfde paragrafen worden de woorden "in artikel 7, §§ 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" telkens vervangen door de woorden "in artikel 15, § 2, van de wet van … tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

3° in paragraaf 3 worden de woorden "of de artikelen 2, eerste lid, 1° en 9° en 15, §§ 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" opgeheven.

4° in dezelfde paragraaf worden de woorden "de artikelen 20, 21, § 1, en 33, van de voormelde wet van 7 april 2019" vervangen door de woorden "de artikel 30 van de voormelde wet van …".

Art. 53

In artikel 16, § 4, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "artikel 17 van de wet van ... betreffende de weerbaarheid van kritieke entiteiten";

et des systèmes d'information d'intérêt général pour la sécurité publique, de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et de l'article 2, alinéa 1er, 1°, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien" sont remplacés par les mots "à l'article 3, 2°, de la loi du ... relative à la résilience des entités critiques".

Art. 52

À l'article 6 de la même loi, les modifications suivantes sont apportées:

1° aux paragraphes 2 et 3, les mots "articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "articles 3, 2°, et 33 de la loi du ... relative à la résilience des entités critiques";

2° dans les même paragraphes, les mots "à l'article 7, §§ 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont chaque fois remplacés par les mots "ou à l'article 15, § 2, de la loi du … établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique";

3° au paragraphe 3, les mots "ou aux articles 2, alinéa 1er, 1° et 9° et 15, §§ 1 à 3, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien" sont supprimés.

4° dans le même paragraphe, les mots "aux articles 20, 21, § 1er, et 33, de la loi précitée du 7 avril 2019" sont remplacés par les mots "à l'article 30 de la loi précitée du …".

Art. 53

À l'article 16, § 4, de la même loi, les modifications suivantes sont apportées:

1° dans l'alinéa 1er, les mots "article 13 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques" sont remplacés par les mots "article 17 de la loi du ... relative à la résilience des entités critiques";

2° in het eerste lid worden de woorden “de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011” vervangen door de woorden “de artikelen 3, 2°, en 33, van de voormelde wet van ...”;

3° in het eerste lid worden de woorden “kritieke infrastructuur” vervangen door de woorden “kritieke entiteit”;

4° in het eerste lid worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van ...”;

5° in het eerste lid worden de woorden “de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en” opgeheven;

6° in het eerste lid worden de woorden “en in artikel 7, §§ 3 en 5, van de voormelde wet van 7 april 2019” opgeheven;

7° in het eerste lid worden de woorden “, een aanbieder van essentiële diensten of een digitaledienstverlener” opgeheven;

8° in het eerste lid worden de woorden “of de voormelde wet van 7 april 2019” opgeheven;

9° in het tweede lid worden de woorden “artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector luchtvervoer en” opgeheven;

10° in het tweede lid worden de woorden “als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, §§ 1 tot 3, van het voormelde koninklijk besluit van 2 december 2011” opgeheven;

11° in het tweede lid worden de woorden “kritieke infrastructuur als bedoeld in dit koninklijk besluit” vervangen door “kritieke entiteit als bedoeld in de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

12° in het derde lid worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” onder 2° vervangen als volgt: “de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

13° in het derde lid worden de woorden “en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer” opgeheven.

2° dans l’alinéa 1er, les mots “articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 précitée” sont remplacés par les mots “articles 3, 2°, et 33 de la loi du ... précitée”;

3° dans l’alinéa 1er, les mots “infrastructure critique” sont remplacés par les mots “entité critique”;

4° dans le premier alinéa, les mots “loi du 1 juillet 2011” sont remplacés par les mots “loi du ...”;

5° dans l’alinéa 1er, les mots “des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique et” sont abrogés;

6° dans l’alinéa 1er, les mots “et à l’article 7, §§ 3 et 5, de la loi précitée du 7 avril 2019” sont abrogés;

7° dans l’alinéa 1er, les mots “, d’un opérateur de services essentiels ou d’un fournisseur de service numérique” sont abrogés;

8° dans l’alinéa 1er, les mots “ou de la loi précitée du 7 avril 2019” sont abrogés;

9° dans l’alinéa 2, les mots “article 11 de l’arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et” sont abrogés;

10° dans l’alinéa 2, les mots “au sens des articles 2, alinéa 1er, 1° et 9°, et 15, §§ 1er à 3, de l’arrêté royal précité du 2 décembre 2011” sont abrogés;

11° dans l’alinéa 2, les mot “infrastructure critique, au sens de cet arrêté royal” sont remplacés par les mots “entité critique, au sens de la loi du ... relative à la résilience des entités critiques”;

12° dans l’alinéa 3, les mots “la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques” sous 2° sont remplacés par les mots: “la loi du ... relative à la résilience des entités critiques”;

13° dans l’alinéa 3, les mots “et de l’arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien” sont abrogés.

Art. 54

In artikel 17, § 3, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden “artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “artikel 18 van de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

2° in het eerste lid worden de woorden “de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011” vervangen door de woorden “de artikelen 3, 2°, en 33, van de voormelde wet van ...”;

3° in het eerste lid worden de woorden “kritieke infrastructuur” vervangen door “kritieke entiteit”;

4° in het eerste lid worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van ...”;

5° in het eerste lid worden de woorden “en de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid” opgeheven;

6° in het eerste lid worden de woorden “en in artikel 7, §§ 3 en 5, van de voormelde wet van 7 april 2019” opgeheven;

7° in het eerste lid worden de woorden “aanbieder van essentiële diensten of digitaledienstverlener” opgeheven;

8° in het eerste lid worden de woorden “of de voormelde wet van 7 april 2019” opgeheven;

9° in het tweede lid worden de woorden “artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector luchtvervoer en” opgeheven;

10° in het tweede lid worden de woorden “als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, §§ 1 tot 3, van het voormelde koninklijk besluit van 2 december 2011” opgeheven;

11° in het tweede lid worden de woorden “kritieke infrastructuur, als bedoeld in artikel 2, 3°, van het voormelde koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer” vervangen door de woorden “kritieke entiteit, zoals bedoeld in artikel 3, 3°, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

Art. 54

À l’article 17, § 3, de la même loi, les modifications suivantes sont apportées:

1° dans l’alinéa 1er, les mots “article 13 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “article 18 de la loi du ... relative à la résilience des entités critiques”;

2° dans l’alinéa 1er, les mots “articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 précitée” sont remplacés par les mots “articles 3, 2°, et 33 de la loi du ... précitée”

3° dans l’alinéa 1er, les mots “infrastructure critique” sont remplacés par les mots “entité critique”;

4° dans l’alinéa 1er, les mots “loi du 1 juillet 2011” sont remplacés par les mots “loi du ...”;

5° dans l’alinéa 1er, les mots “et des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique” sont abrogés;

6° dans l’alinéa 1er, les mots “et à l’article 7, §§ 3 et 5, de la loi précitée du 7 avril 2019” sont abrogés;

7° dans l’alinéa 1er, les mots “, d’un opérateur de services essentiels ou d’un fournisseur de service numérique” sont abrogés;

8° dans l’alinéa 1er, les mots “ou de la loi précitée du 7 avril 2019” sont abrogés;

9° dans l’alinéa 2, les mots “article 11 de l’arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et” sont abrogés;

10° dans l’alinéa 2, les mots “au sens des articles 2, alinéa 1er, 1° et 9°, et 15, §§ 1er à 3, de l’arrêté royal précité du 2 décembre 2011” sont abrogés;

11° dans l’alinéa 2, les mot “infrastructure critique, visée à l’article 2, 3° de l’arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien” sont remplacés par les mots “entité critique, visée à l’article 3, 3°, de la loi du ... relative à la résilience des entités critiques”;

12° in lid 3, in de bepaling onder 2° worden de woorden ", de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" opgeheven;

13° in het derde lid worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" onder 2° vervangen als volgt: "de wet van ... betreffende de weerbaarheid van kritieke entiteiten";

14° in het derde lid worden de woorden "en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" opgeheven.

Art. 55

In artikel 36, § 1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in 4° worden de woorden "de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, §§ 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "de artikelen 3, 2°, en 33, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten of de artikel 15, § 2, van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

2° in de bepaling onder 4° worden de woorden "en 15, §§ 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" opgeheven;

3° in 4° worden de woorden "in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, van de voormelde wet van 7 april 2019" vervangen door de woorden "in artikelen 15, § 2, en 24 van de voormelde wet van …".

12° dans l'alinéa 3, le 2°, les mots ", de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont abrogés;

13° dans l'alinéa 3, les mots "la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques" sous 2° sont remplacés par les mots "la loi du ... relative à la résilience des entités critiques";

14° dans l'alinéa 3, les mots "et de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien" sont abrogés.

Art. 55

À l'article 36, § 1er, de la même loi, les modifications suivantes sont apportées:

1° dans le 4°, les mots "articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, à l'article 7, §§ 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" sont remplacés par les mots "articles 3, 2°, et 33, de la loi du ... relative à la résilience des entités critiques ou à l'article 15, § 2, de la loi du […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique";

2° dans le 4°, les mots "en 15, §§ 1 à 3, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien" sont abrogés;

3° dans le 4°, les mots "aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, de la loi précitée du 7 avril 2019" sont remplacés par les mots "aux articles 15, § 2, et 24 de la loi précitée du …".

Afdeling 3

Wijziging van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 56

In artikel 14 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, laatstelijk gewijzigd bij wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, worden de volgende wijzigingen aangebracht:

a) in de eerste zin worden de woorden “met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren” vervangen door de woorden “met betrekking tot de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, in de zin van de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

b) in de bepaling onder 3°, wordt de bepaling onder g) vervangen als volgt:

“de wet van ... betreffende de weerbaarheid van kritieke entiteiten, wat de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, betreft”;

2° de paragraaf 2, 7°, wordt opgeheven.

Afdeling 4

Wijziging van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 57

In artikel 36/14 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, worden in de bepaling onder 20° de woorden “artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren zulks vereist” vervangen door de woorden “artikel 26 van de wet van ... betreffende de weerbaarheid van kritieke entiteiten zulks vereist”.

Section 3

Modification de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications

Art. 56

À l’article 14 de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications, modifiée en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 1er, les modifications suivantes sont apportées:

a) dans la première phrase, les mots “en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques aux sens de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “relevant du secteur des infrastructures numériques, à l’exception des fournisseurs de services de confiance, au sens de la loi du ... relative à la résilience des entités critiques”;

b) dans la disposition sous le 3°, le g) est remplacé comme suit:

“la loi du ... relative à la résilience des entités critiques, en ce qui concerne le secteur de l’infrastructure numérique, à l’exception des fournisseurs de services de confiance”;

2° le paragraphe 2, 7°, est abrogé.

Section 4

Modification de la loi du 22 février 1998 portant le statut organique de la Banque nationale de Belgique

Art. 57

À l’article 36/14 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, dans le 20°, les mots “l’article 19 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques l’exige” sont remplacés par les mots “l’article 26 de la loi du ... relative à la résilience des entités critiques l’exige”.

Art. 58

In artikel 36/49 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “kritieke infrastructuur” worden vervangen door de woorden “kritieke entiteit”;

2° de woorden “wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren” worden vervangen door de woorden “wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 5

Wijziging van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen

Art. 59

In artikel 15/2*sexies*, § 3, van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in 4° worden de woorden “kritieke nationale infrastructuur” vervangen door de woorden “kritieke entiteit”;

2° in 4° worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 6

Wijziging van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt

Art. 60

In artikel 14/1, § 3, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in 4° worden de woorden “kritieke nationale infrastructuur” vervangen door de woorden “kritieke entiteit”;

2° in 4° worden de woorden “de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren” vervangen door de woorden “de wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Art. 58

À l’article 36/49 de la même loi, les modifications suivantes sont apportées:

1° les mots “infrastructures critiques” sont remplacés par les mots “entités critiques”;

2° les mots “loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “loi du ... relative à la résilience des entités critiques”.

Section 5

Modification de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations

Art. 59

À l’article 15/2*sexies*, § 3, de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, modifiée en dernier lieu par la loi du 31 juillet 2017, les modifications suivantes sont apportées:

1° dans le 4°, les mots “infrastructure nationale critique” sont remplacés par les mots “entité critique”;

2° dans le 4°, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du ... relative à la résilience des entités critiques”.

Section 6

Modification de la loi du 29 avril 1999 relative à l’organisation du marché de l’électricité

Art. 60

À l’article 14/1, § 3, de la loi du 29 avril 1999 relative à l’organisation du marché de l’électricité, modifiée en dernier lieu par la loi du 31 juillet 2017, les modifications suivantes sont apportées:

1° dans le 4°, les mots “infrastructure nationale critique” sont remplacés par les mots “entité critique”;

2° dans le 4°, les mots “la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “la loi du ... relative à la résilience des entités critiques”.

Afdeling 7

Wijziging van het Strafwetboek

Art. 61

In artikel 546/2, § 1, van het Strafwetboek, ingevoegd bij wet van 20 mei 2016, wordt 6° vervangen als volgt:

“6° Indien een kritieke entiteit, in de zin van de wet van ... betreffende de weerbaarheid van kritieke entiteiten werd binnengegaan of binnengedrongen”.

Art. 62

In artikel 550*ter*, § 1, van het Strafwetboek, ingevoegd bij wet van 28 november 2000 en gewijzigd bij de wet van 6 juli 2017, wordt het derde lid vervangen als volgt:

“Dezelfde straf wordt toegepast wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt tegen een informatiesysteem van een kritieke entiteit zoals bedoeld in artikel 3, 3°, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Afdeling 8

Wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 63

In artikel 15*bis*, lid 1, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, ingevoegd door de wet van 7 april 2019, worden de volgende wijzigingen aangebracht:

1°) de woorden “artikel 24 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren” worden vervangen door de woorden “artikel 33 van de wet van ... betreffende de weerbaarheid van kritieke entiteiten”;

2°) de woorden “aangeduid als kritieke infrastructuur krachtens bovengenoemde wet van 1 juli 2011” worden vervangen door de woorden “aangeduid als kritieke entiteit krachtens de wet van ... betreffende de weerbaarheid van kritieke entiteiten”.

Section 7

Modification du Code pénal

Art. 61

À l’article 546/2, § 1er, du Code pénal, inséré par la loi du 20 mai 2016, le 6° est remplacé comme suit:

“6° Si une entité critique, au sens de la loi du ... sur la résilience des entités critiques, a fait l’objet d’une entrée ou d’une intrusion”.

Art. 62

À l’article 550*ter*, § 1er, du Code pénal, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juillet 2017, l’ alinéa 3 est remplacé par ce qui suit:

“La même peine est appliquée lorsque l’infraction visée à l’alinéa 1er est commise à l’encontre d’un système d’information d’une entité critique telle que visée à l’article 3, 3°, de la loi du ... relative à la résilience des entités critiques”.

Section 8

Modification de la loi du 15 avril 1994 relative à la protection de la population et de l’environnement contre les dangers résultant des rayonnements ionisants et relative à l’Agence fédérale de Contrôle nucléaire

Art. 63

À l’article 15*bis*, alinéa 1er, de la loi du 15 avril 1994 relative à la protection de la population et de l’environnement contre les dangers résultant des rayonnements ionisants et relative à l’Agence fédérale de Contrôle nucléaire, inséré par la loi du 7 avril 2019, les modifications suivantes sont apportées:

1°) les mots “l’article 24 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques” sont remplacés par les mots “l’article 33 de la loi du ... relative à la résilience des entités critiques”;

2°) les mots “désignés comme infrastructure critique en vertu de la loi du 1er juillet 2011 susmentionnée” sont remplacés par les mots “désignés comme entité critique en vertu de la loi du ... relative à la résilience des entités critiques”.

Afdeling 9

Wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging

Art. 64

Artikel 6, § 1, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, gewijzigd bij de wet van 31 mei 2022, wordt aangevuld met een lid luidende:

"Onverminderd de verplichtingen opgenomen in de internationale instrumenten die hen binden, zijn de ondersteunende diensten verplicht om ambtshalve of op verzoek van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en de inlichtingen waarover zij beschikken in het kader van hun wettelijke opdrachten en die relevant blijkt met het oog op de verwezenlijking van de doelstellingen van de dreigingsanalyse als bedoeld in artikel 9, § 2, van de wet van ... betreffende de weerbaarheid van kritieke entiteiten, te communiceren."

Afdeling 10

Wijziging van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Art. 65

In artikel 3, § 4, van de wet van … tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid worden de woorden "exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "kritieke entiteiten als bedoeld in de wet van … betreffende de weerbaarheid van kritieke entiteiten".

Art. 66

In artikel 8 van dezelfde wet wordt de bepaling onder 43° vervangen door:

"43° wet van …: de wet van … betreffende de weerbaarheid van kritieke entiteiten".

Section 9

Modification de la loi du 10 juillet 2006 relative à l'analyse de la menace

Art. 64

L'article 6, § 1er, de la loi du 10 juillet 2006 relative à l'analyse de la menace, modifié par la loi du 31 mai 2022, est complété par un alinéa rédigé comme suit:

"Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'article 9, § 2, de la loi du ... relative à la résilience des entités critiques.".

Section 10

Modification de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Art. 65

Dans l'article 3, § 4, de la loi du … établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les mots "exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques" sont remplacés par les mots "entités critiques au sens de la loi du … relative à la résilience des entités critiques".

Art. 66

Dans l'article 8 de la même loi, le 43° est remplacé par ce qui suit:

"43° loi du …: la loi du … relative à la résilience des entités critiques".

Art. 67

In artikel 15, § 2, tweede lid, van dezelfde wet worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van …”.

Art. 68

In artikel 25 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in paragraaf 2 worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van …”;

2° in paragraaf 4 wordt “wet van 1 juli 2011” vervangen door “wet van …”;

3° in dezelfde paragraaf worden de woorden “exploitanten van infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt” vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van …”.

Art. 69

In artikel 28, § 2, 7°, van dezelfde wet worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van …”.

Art. 70

In artikel 37, § 5, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “wet van 1 juli 2011” worden vervangen door de woorden “wet van …”;

2° de woorden “exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt” worden vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van …”.

Art. 71

In artikel 40, § 1, tweede lid, van dezelfde wet worden de woorden “exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011” vervangen door de woorden “kritieke entiteiten als bedoeld in de wet van …”.

Art. 67

Dans l’article 15, § 2, alinéa 2, de la même loi, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”.

Art. 68

À l’article 25 de la même loi, les modifications suivantes sont apportées:

1° dans le paragraphe 2, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”;

2° dans le paragraphe 4, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”;

3° dans le même paragraphe, les mots “exploitants d’infrastructures recensées en tant qu’infrastructures critiques en vertu de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du ….

Art. 69

Dans l’article 28, § 2, 7°, de la même loi, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”.

Art. 70

À l’article 37, § 5, de la même loi, les modifications suivantes sont apportées:

1° les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”;

2° les mots “exploitants d’infrastructures identifiées comme infrastructures critique en vertu de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du …”.

Art. 71

Dans l’article 40, § 1er, alinéa 2, de la même loi, les mots “exploitants d’une infrastructure critique au sens de la loi du 1er juillet 2011” sont remplacés par les mots “entités critiques au sens de la loi du …”.

Art. 72

In artikel 45, § 1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden “dat een exploitant van een infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur wordt geïdentificeerd” worden vervangen door de woorden “dat een kritieke entiteit zoals bedoeld in de wet van …”;

2° de woorden “een exploitant van een infrastructuur die is aangemerkt als kritieke infrastructuur uit hoofde van de wet van 1 juli 2011” worden vervangen door de woorden “een kritieke entiteit als bedoeld in de wet van …”;

3° de woorden “wet van 1 juli 2011” worden telkens vervangen door de woorden “wet van …”.

Art. 73

In artikel 67, 5°, van dezelfde wet worden de woorden “wet van 1 juli 2011” telkens vervangen door de woorden “wet van …”.

Art. 74

In artikel 68, 5°, van dezelfde wet worden de woorden “wet van 1 juli 2011” vervangen door de woorden “wet van …”.

HOOFDSTUK 10

Slotbepalingen

Art. 75

De Koning kan, bij een in Ministerraad overlegd besluit, de bepalingen van hoofdstukken 4 tot en met 7 en de uitvoeringsbesluiten ervan volledig of gedeeltelijk van toepassing maken op andere sectoren dan diegene bedoeld in de bijlage.

Art. 76

De wet van 1 juli 2011 betreffende de bescherming en beveiliging van kritieke infrastructuren wordt opgeheven.

Art. 72

À l’article 45, § 1er, de la même loi, les modifications suivantes sont apportées:

1° les mots “qu’un exploitant d’une infrastructure identifiée comme critique en vertu de la loi du 1er juillet 2011” sont remplacés par les mots “qu’une entité critique au sens de la loi du …”;

2° les mots “d’un exploitant d’une infrastructure qui est définie comme infrastructure critique en vertu de la loi du 1er juillet 2011” sont remplacé par les mots “d’une entité critique au sens de la loi du …”;

3° les mots “loi du 1er juillet 2011” sont à chaque fois remplacés par les mots “loi du …”.

Art. 73

Dans l’article 67, 5°, de la même loi, les mots “loi du 1er juillet 2011” sont à chaque fois remplacés par les mots “loi du …”.

Art. 74

Dans l’article 68, 5°, de la même loi, les mots “loi du 1er juillet 2011” sont remplacés par les mots “loi du …”.

CHAPITRE 10

Dispositions finales

Art. 75

Le Roi peut, par arrêté délibéré en Conseil des ministres, rendre applicables en tout ou en partie les dispositions des chapitres 4 à 7 inclus et les arrêtés d’exécution à d’autres secteurs que ceux visés en annexe.

Art. 76

La loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques est abrogée.

Art. 77

§ 1. Entiteiten die op grond van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren werden aangeduid als exploitanten van een Europese of nationale kritieke infrastructuur, worden op 17 juli 2026 van rechtswege beschouwd als kritieke entiteiten zoals bedoeld in artikel 11 van deze wet.

De lijst van kritieke infrastructuren zoals opgesteld volgens de wet van 1 juli 2011 zal, behoudens aanpassingen, voldoen aan artikel 11 van deze wet.

§ 2. De entiteiten bedoeld in paragraaf 1, lid 1, blijven tot 17 mei 2027 gehouden aan de verplichtingen uit de artikelen 13, 13/1, 13/2, 14, 24 en 25 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren, zoals deze op dat ogenblik van toepassing waren.

Art. 78

Met uitzondering van sectoren waarin nog geen kritieke entiteiten waren aangewezen voor de inwerkingtreding van deze wet, worden alle dreigingsanalyses geacht geldig te zijn voor een periode van maximaal vier jaar, overeenkomstig artikel 8, zelfs indien de datum waarop zij werden uitgevoerd voor de inwerkingtreding van deze wet valt.

Art. 79

Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Gegeven te Brussel, 11 september 2025

FILIP

VAN KONINGSWEGE:

De eerste minister,

Bart De Wever

De minister van Economie en Landbouw,

David Clarinval

Art. 77

§ 1er. Les entités qui ont été désignées comme exploitants d'une infrastructure critique européenne ou nationale en vertu de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques seront automatiquement considérées le 17 juillet 2026 comme des entités critiques au sens de l'article 11 de la présente loi.

La liste des infrastructures critiques telle qu'établie par la loi du 1er juillet 2011 sera conforme à l'article 11 de cette loi, sous réserve d'adaptations.

§ 2. Les entités visées au paragraphe 1er, alinéa 1er, restent tenues par les obligations énoncées aux articles 13, 13/1, 13/2, 14, 24 et 25 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques jusqu'au 17 mai 2027, telles qu'applicables à ce moment-là.

Art. 78

À l'exception des secteurs dans lesquels aucune entité critique n'avait encore été désignée avant l'entrée en vigueur de la présente loi, toutes les analyses de la menace sont réputées valables pendant une durée maximale de quatre ans, en vertu de l'article 8 et cela, même si la date à laquelle elles sont été effectuées est antérieure à l'entrée en vigueur de la présente loi.

Art. 79

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Donné à Bruxelles, le 11 septembre 2025

PHILIPPE

PAR LE ROI:

Le premier ministre,

Bart De Wever

Le ministre de l'Économie et de l'Agriculture,

David Clarinval

De minister van Volksgezondheid,

Frank Vandenbroucke

De minister van Financiën,

Jan Jambon

De minister van Justitie, belast met de Noordzee,

Annelies Verlinden

De minister van Veiligheid en Binnenlandse Zaken,

Bernard Quintin

De minister van Mobiliteit,

Jean-Luc Crucke

De minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid,

Vanessa Matz

De minister van Energie,

Mathieu Bihet

De minister van Middenstand, Zelfstandigen en Kmo's,

Eléonore Simonet

Le ministre de la Santé publique,

Frank Vandenbroucke

Le ministre des Finances,

Jan Jambon

La ministre de la Justice, chargée de la Mer du Nord,

Annelies Verlinden

Le ministre de la Sécurité et de l'Intérieur,

Bernard Quintin

Le ministre de la Mobilité,

Jean-Luc Crucke

La ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique,

Vanessa Matz

Le ministre de l'Énergie,

Mathieu Bihet

La ministre des Classes moyennes, des Indépendants et des PME,

Eléonore Simonet

BIJLAGE

Sector	Deelsector	Categorie van entiteit	Sectorale overheid
1. Energie	Elektriciteit	Elektriciteitsbedrijven als bedoeld in art. 2, punt 57, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad, die de functie verrichten van "levering" in de zin van artikel 2, punt 12, van die richtlijn	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Distributiesysteembeheerders als bedoeld in art. 2, punt 29, van Richtlijn (EU) 2019/944	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 35, van Richtlijn (EU) 2019/944	
		Producenten als bedoeld in art. 2, punt 38, van Richtlijn (EU) nr. 2019/944	
		Benoemde elektriciteitsmarktbeheerders als bedoeld in art. 2, punt 8, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad	
		Marktdeelnemers als bedoeld in art. 2, punt 25, van Verordening (EU) 2019/943, die diensten verlenen op het gebied van aggregatie, vraagrespons of energieopslag als bedoeld in art. 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944	
	Olie	Exploitanten van oliepijpleidingen	
		Exploitanten van voorzieningen voor de productie, raffinage, behandeling, opslag en transmissie van olie	
		Centrale entiteiten voor de voorraadvorming als bedoeld in art. 2, punt f), van Richtlijn 2009/119/EG van de Raad	
	Gas	Leveringsbedrijven als bedoeld in art. 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad	
		Distributiesysteembeheerders als bedoeld in art. 2, punt 6, van Richtlijn 2009/73/EG	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 4, van Richtlijn 2009/73/EG	
		Opslagsysteembeheerders als bedoeld in art. 2, punt 10, van Richtlijn 2009/73/EG	
		LNG-systeembeheerders als bedoeld in art. 2, punt 12, van Richtlijn 2009/73/EG	
		Aardgasbedrijven als bedoeld in art. 2, punt 1, van Richtlijn 2009/73/EG	
		Exploitanten van voorzieningen voor de productie, opslag en transmissie van aardgas	

	Stadsverwarming- en koeling	Exploitanten van stadsverwarming of stadskoeling als bedoeld in art. 2, punt 19, van Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad	
	Waterstof	Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof	
2. Vervoer	Lucht	Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) 300/2008, die voor commerciële doeleinden worden gebruikt	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, Richtlijn 2009/12/EG van het Europees Parlement en de Raad; luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de tot het kernnetwerk behorende luchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad zijn opgenomen, alsook de entiteiten die bijhorende installaties bedienen welke zich op de luchthavens bevinden	
		Luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad	
	Spoor	Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, Richtlijn 2012/34/EU van het Europees Parlement en de Raad	
		Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2012/34/EU, en exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die Richtlijn	
	Water	Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht zoals voor maritiem transport gedefinieerd in bijlage I bij Verordening (EG) 725/2004, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen	
		Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2005/65/EG, incl. hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, Verordening (EG) 725/2004, alsook entiteiten die werken en uitrusting in havens beheren	
		Exploitanten van verkeersbegeleidingssystemen (VTS) zoals gedefinieerd in artikel 3, punt o), van Richtlijn 2002/59/EG van het Europees Parlement en de Raad	
	Weg	Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1 van Richtlijn 2010/40/EU van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, Verordening (EU) 2015/962 van de Commissie die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties voor wie verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteiten is	
	Openbaar vervoer	Exploitanten van openbare diensten zoals gedefinieerd in artikel 2, punt d), Verordening (EG) 1370/2007 van het	**De Overheid aangewezen door de Koning bij besluit**

		Europees Parlement en de Raad, met uitzondering van de entiteiten die reeds door een andere deelsector gevat worden	**vastgesteld na overleg in de Ministerraad**
3. Bankwezen		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) 575/2013	**De Nationale Bank van België (NBB)**
4. Infrastructuur voor de financiële markt		Centrale tegenpartijen (CTP's) zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) 648/2012	**De Nationale Bank van België (NBB)**
		Beheerders van handelsplatforms zoals gedefinieerd in artikel 4, punt 24, Richtlijn 2014/65/EU	**De Autoriteit voor Financiële Diensten en Markten (FSMA)**
5. Digitale infrastructuur		Aanbieders van internetknooppunten zoals gedefinieerd in artikel 6, punt 18 van Richtlijn (EU) 2022/2555	**Het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.)**
		DNS-dienstverleners zoals gedefinieerd in artikel 6, punt 20, van Richtlijn (EU) 2022/2555, met uitzondering van exploitanten van root-naamservers	
		Registers voor topleveldomeinnamen zoals gedefinieerd in artikel 6, punt 21 van Richtlijn (EU) 2022/2555	
		Aanbieders van openbare elektronische-communicatienetwerken zoals gedefinieerd in art. 2, punt 8, van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad	
		Aanbieders van elektronische-communicatiediensten als bedoeld in art. 2, punt 4, van Richtlijn (EU) 2018/1972, voor zover hun diensten publiek beschikbaar zijn.	
		Aanbieders van netwerken voor content delivery zoals gedefinieerd in artikel 6, punt 32, van Richtlijn 2022/2555	
		Aanbieders van datacentrumdiensten zoals gedefinieerd in artikel 6, punt 31, van Richtlijn 2022/2555	
		Aanbieders van cloudcomputingdiensten zoals gedefinieerd in artikel 6, punt 30, van Richtlijn 2022/2555	
		Verleners van vertrouwensdiensten zoals gedefinieerd in artikel 3, punt 19, van Verordening (EU) 910/2014 van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in art. 2, punt 1, a), Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad, maar met uitzondering van distributeurs voor wie de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
7. Afvalwater		Ondernemingen die stedelijk, huishoudelijk en industrieel afvalwater zoals gedefinieerd in art. 2, punten 1, 2 en 3, Richtlijn 91/271/EEG van de Raad opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk, huishoudelijk en industrieel	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**

		afvalwater slechts een niet essentieel onderdeel van hun algemene activiteit is	
8. Volksgezondheid		Zorgaanbieders zoals gedefinieerd in art. 3, punt g), Richtlijn 2011/24/EG van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		EU-referentielaboratoria zoals gedefinieerd in art. 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
		Entiteiten die zich bezighouden met onderzoek naar en de ontwikkeling van geneesmiddelen zoals gedefinieerd in art. 1, punt 2, Richtlijn 2001/83/EG van het Europees Parlement en de Raad	**Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG)**
		Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen zoals gedefinieerd in sectie C, afd. 21, van NACE rev. 2 vervaardigen	
		Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") zoals gedefinieerd in art. 22 Verordening (EU) 2022/123 van het Europees Parlement en de Raad	
		Entiteiten die houder zijn van een groothandelsvergunning zoals gedefinieerd in art. 79 Richtlijn 2001/83/EG	
9. Overheid		Overheidsinstanties van die van de Federale staat afhangen, met uitzondering van de rechterlijke macht, parlementen en centrale banken	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
10. Ruimtevaart		Exploitanten van grondfaciliteiten die in het bezit zijn van en beheerd en geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische communicatie netwerken zoals gedefinieerd in art. 2, punt 8 Richtlijn (EU) 2018/1972	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**
11. Productie, verwerking en distributie van levensmiddelen		Levensmiddelenbedrijven zoals gedefinieerd in punt 2) van artikel 3 van Verordening (EG) nr. 178/20021 van het Europees Parlement en de Raad die zich uitsluitend bezighouden met logistiek en groothandel, en met grootschalige industriële productie en verwerking	**De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad**

Gezien om gevoegd te worden bij de wet van…. betreffende de weerbaarheid van kritieke entiteiten

Brussel, 11 september 2025.

FILIP

VAN KONINGSWEGE:

De eerste minister,

Bart De Wever

De minister van Economie en Landbouw,

David Clarinval

De minister van Volksgezondheid,

Frank Vandenbroucke

De minister van Financiën,

Jan Jambon

De minister van Justitie, belast met de Noordzee,

Annelies Verlinden

De minister van Veiligheid en Binnenlandse Zaken,

Bernard Quintin

De minister van Mobiliteit,

Jean-Luc Crucke

De minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid,

Vanessa Matz

De minister van Energie,

Mathieu Bihet

De minister van Middenstand, Zelfstandigen en Kmo's,

Eléonore Simonet

ANNEXE

Secteur	Sous-secteur	Categorie d'entité	Autorité sectorielle
1. Énergie	Électricité	Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil, qui assurent la fonction de "fourniture" au sens de l'article 2, point 12), de ladite Directive	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944	
		Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944	
		Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944	
		Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil	
		Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943, qui fournissent des services d'agrégation, de participation active de la demande ou de stockage de l'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944	
	Pétrole	Exploitants d'oléoducs	
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole	
		Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil	
	Gaz	Entreprises de fourniture au sens de l'article 2, point 8), de la directive 2009/73/CE du Parlement européen et du Conseil	
		Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE	
		Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE	
		Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la directive 2009/73/CE	
		Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE	
		Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE	
		Exploitants d'installations de raffinage et de traitement de gaz naturel	

	Réseaux de chaleur et de froid	Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil	
	Hydrogène	Exploitants des systèmes de production, de stockage et de transport d'hydrogène	
2. Transports	Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 utilisés à des fins commerciales	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du conseil, aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports	
		Services du contrôle de la circulation aérienne assurant les services de contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil	
	Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil	
		Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, et exploitants d'installations de services au sens de l'article 3, point 12), de ladite directive	
	Transports maritimes	Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret qu'elles sont définies pour la domaine du transport maritime au sens de l'Annexe I du règlement (CE) n° 725/2004, à l'exclusion des navires exploités à titre individuel par ces sociétés	
		Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports	
		Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil	
	Transports routiers	Systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
		Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation des systèmes de transport intelligents constituent une partie non essentielle de leur activité générale	
	Transport public	Opérateurs de services publics au sens de l'article 2 point (d) du règlement (CE) n° 1370/2007 du Parlement européen et du	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**

		Conseil, à l'exception des entités qui relèvent déjà d'un autre sous-secteur	
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du Règlement (UE) n° 575/2013 du Parlement européen et du Conseil	**La Banque nationale de Belgique (BNB)**
4. Infrastructures de marchés financiers		Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012	**La Banque nationale de Belgique (BNB)**
		Opérateurs de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE	**L'autorité des services et marchés financiers (FSMA)**
5. Infrastructures numériques		Fournisseurs de points d'échange internet au sens de l'article 6, point 18), de la directive (UE) 2022/2555	**Institut belge des services postaux et des télécommunications (I.B.P.T.)**
		Fournisseurs de services DNS au sens de l'article 6, point 20), de la directive (UE) 2022/2555, à l'exclusion des opérateurs de serveurs racines de noms de domaines	
		Registres de noms de domaines de premier niveau au sens de l'article 6, point 21), de la directive (UE) 2022/2555	
		Fournisseurs de services de centre de données au sens de l'article 6, point 31), de la directive (UE) 2022/2555	
		Fournisseurs de réseaux de diffusion de contenu au sens de l'article 6, point 32), de la directive (UE) 2022/2555	
		Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972 du Parlement européen et du Conseil	
		Fournisseurs de services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 dans la mesure où leurs services sont accessibles au public	
		Fournisseurs de services d'informatique en nuage au sens de l'article 6, point 30), de la directive (UE) 2022/2555	
		Prestataires de services de confiance au sens de l'article 3, point 19), du règlement (UE) nº 910/2014 du Parlement européen et du conseil	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
7. Eaux résiduaires		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, des eaux ménagères usées et des eaux industrielles usées au sens de l'article 2, points 1) à 3), de la directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**

8. Santé		Prestataire de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
		Laboratoires de référence de l'Union européenne au sens l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil	**Agence fédérale des médicaments et des produits de santé (A.F.M.P.S.)**
		Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la section C, division 21, de la NACE Rév. 2	
		Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique ("liste des dispositifs médicaux critiques en cas d'urgence de santé publique") au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil	
		Entités titulaires d'une autorisation de distribution au sens de l'article 79 de la directive 2001/83/CE	
9. Administrations publiques		Administrations publiques des pouvoirs publics centraux,– excluant le pouvoir juridique, les parlements, et les banques centrales	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
10. Espace		Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**
11. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3 point 2 du règlement (CE) n°178/2021 du Parlement européen et du Conseil qui exercent exclusivement des activités de logistique et de distribution en gros ainsi que de production et de transformation à grande échelle	**L'autorité désignée par le Roi par arrêté délibéré en Conseil des ministres**

Vu pour être annexé à la loi du …. relative à la résilience des entités critiques

Bruxelles, le 11 septembre 2025.

PHILIPPE

PAR LE ROI:

Le premier ministre,

Bart De Wever

Le ministre de l'Économie et de l'Agriculture,

David Clarinval

Le ministre de la Santé publique,

Frank Vandenbroucke

Le ministre des Finances,

Jan Jambon

La ministre de la Justice, chargée de la Mer du Nord,

Annelies Verlinden

Le ministre de la Sécurité et de l'Intérieur,

Bernard Quintin

Le ministre de la Mobilité,

Jean-Luc Crucke

La ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique,

Vanessa Matz

Le ministre de l'Énergie,

Mathieu Bihet

La ministre des Classes moyennes, des Indépendants et des PME,

Eléonore Simonet

CONCORDANTIETABEL

RICHTLIJN – WETSONTWERP

Artikels uit de Richtlijn (EU) 2022/2557 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG (I)		Artikels uit het wetsontwerp	Commentaar
Art. 1	(1)	-	Bepaling dient niet omgezet te worden – onderwerp van de Richtlijn
	(2)	Art. 6, § 1	
	(3)	Art. 6, § 2	
	(4)	Art. 23	
	(5)	-	
	(6)	Art. 7, § 1	
	(7)	Art. 7, § 2	
	(8)	-	
	(9)	-	
Art. 2	(1)	Art. 3, 3°	
	(2)	Art. 3, 4°	
	(3)	Art. 3, 5°	

	(4)	Art. 3, 6°	
	(5)	Art. 3, 7°	
	(6)	Art. 3, 8°	
	(7)	Art. 3, 9°	
	(8)	-	Deze definitie wordt niet omgezet omdat het begrip niet gebruikt wordt in het ontwerp van wet. Het begrip wordt overigens enkel gebruikt in artikel 16 van de Richtlijn waarin staat dat de lidstaten, waar nuttig en zonder het gebruik van een bepaalde soort technologie op te leggen of te bevoorrechten, het gebruik aanmoedigen van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiligings- en weerbaarheidsmaatregelen die van toepassing zijn op de kritieke entiteiten.
	(9)	-	Zie hierboven, art. 2, (8)
	(10)	Art. 3, 11°; bijlage	
Art. 3		-	Bepaling dient niet omgezet te worden – het betreft het principe van minimumharmonisatie van de richtlijn
Art. 4	(1)	Art. 22, lid 1 en lid 3	
	(2)	Art. 22, lid 4	
	(3)	Art. 21, § 2	Rapportage van de strategie aan Europese Commissie door lidstaten: de bevoegde autoriteit voldoet aan alle rapportageverplichtingen die voortvloeien uit hoofde van de Richtlijn.

Art. 5	(1)	Art. 8, §§ 1 - 3	
	(2)	Art. 8, § 4	
	(3)	Art. 8, § 2	
	(4)	Art. 21, § 2	Rapportage aan Europese Commissie: de bevoegde autoriteit voldoet aan alle rapportageverplichtingen die voortvloeien uit hoofde van de Richtlijn.
	(5)	-	Betreft de mogelijkheid voor de Europese Commissie om een vrijwillig gemeenschappelijk rapportagemodel op te stellen waardoor het niet moet worden omgezet.
Art. 6	(1)	Art. 12, § 3	
	(2)	Art. 10, § 1; Art. 11, § 1	
	(3)	Art. 13, § 1; Art. 18, § 4	
	(4)	Art. 12, § 4	
	(5)	Art. 12, § 3	
	(6)	-	Deze bepaling dient niet omgezet te worden aangezien het de mogelijkheid voorziet dat de Europese Commissie aanbevelingen en niet-bindende richtsnoeren opstelt om de lidstaten te helpen bij het identificeren van kritieke entiteiten.
Art. 7	(1)	Art. 11, § 2	
	(2)	Art. 21, § 2	Rapportage aan de Europese Commissie door de lidstaten na identificatie van kritieke entiteiten: de bevoegde autoriteit voldoet

			aan alle rapportageverplichtingen die voortvloeien uit hoofde van de Richtlijn.
	(3)	-	Deze bepaling dient niet omgezet te worden: de Europese Commissie stelt niet-bindende richtsnoeren vast om de toepassing van de criteria uit artikel 7, lid 1 te vergemakkelijken.
Art. 8		Art. 6, § 1	Artikel 5, § 1 bepaalt dat wanneer kritieke entiteiten uit de sectoren bankwezen, financiële marktinfrastructuur en digitale infrastructuur op basis van andere wetgeving gelijkwaardige maatregelen dienen te nemen of hebben genomen, hoofdstuk 4, afdeling 2, hoofdstuk 5 en hoofdstuk 7 niet op die kritieke entiteiten van toepassing zijn.
Art. 9	(1)	Art. 3, 2°; Bijlage	De sectorale overheden worden aangeduid als bevoegde autoriteit voor de in bijlage vermelde sectoren die onder hun bevoegdheid vallen.
	(2)	Art. 21, § 1	Er wordt een delegatie gegeven aan de Koning om het nationaal centraal contactpunt aan te duiden.
	(3)	-	Rapportage betreffende meldingen van incidenten aan Europese Commissie: de bevoegde autoriteit voldoet aan alle rapportageverplichtingen die voortvloeien uit hoofde van de Richtlijn. Daarnaast betreft deze bepaling ook een verplichting voor de Europese Commissie om een gemeenschappelijk rapportagemodel te ontwikkelen.
	(4)	-	Deze bepaling dient niet omgezet te worden: de lidstaat moet zorgen voor de nodige bevoegdheden en toereikende financiële middelen om de hun toegewezen taken op doeltreffende en efficiënte wijze uit te voeren.

	(5)	Art. 25	Lidstaat zorgt dat de bevoegde autoriteit overlegt en samenwerkt met andere betrokken nationale autoriteiten.
	(6)	Art. 25	
	(7)	-	Bepaling betreft uitsluitend een verplichting van de lidstaten ten aanzien van de Europese Commissie en dient derhalve geen onderwerp uit te maken van een omzetting.
	(8)	-	Bepaling dient niet omgezet te worden aangezien het uitsluitend een verplichting voor de Europese Commissie bevat.
Art. 10	(1)	Art. 21, § 3	De coördinerende rol van de bevoegde nationale autoriteit, dewelke wordt aangeduid door de Koning, zal verder uitgewerkt worden in een uitvoeringsbesluit. Deze rol betreft de facilitatie van informatie-uitwisseling en samenwerking tussen alsook de ondersteuning van de bevoegde autoriteiten bij het uitvoeren van de verplichtingen uit hoofde van deze richtlijn.
	(2)	Art. 21, § 3	
	(3)	Art. 24	
Art. 11	(1)	Art. 15	
	(2)	Art. 15	
Art. 12	(1)	Art. 17, § 1, lid 1	
	(2)	Art. 17, § 1, lid 2 en § 2	
Art. 13	(1)	Art. 18, §§ 1-2	

	(2)	Art. 18, § 4	
	(3)	Art. 16	Deze bepaling legt de verplichting op voor elke kritieke entiteit om een verbindingsfunctionaris of een gelijkwaardige functionaris aan te wijzen als het contactpunt met de bevoegde autoriteiten: De keuze werd gemaakt voor een contactpunt dat vierentwintig op vierentwintig uur bereikbaar is. Het komt toe aan de kritieke entiteit om te waken over een permanentie die gewaarborgd wordt door een of meerdere personen gemachtigd om vragen betreffende de weerbaarheid van de kritieke entiteit te behandelen.
	(4)	-	Bepaling dient niet omgezet te worden aangezien het uitsluitend een verplichting voor de Europese Commissie bevat.
	(5)	-	Bepaling dient niet omgezet te worden aangezien het uitsluitend een verplichting voor de Europese Commissie bevat.
	(6)	-	Bepaling dient niet omgezet te worden aangezien het uitsluitend een verplichting voor de Europese Commissie bevat.
Art. 14	(1)	Art. 19	De veiligheidsverificatie zoals bedoeld in deze bepaling maakt reeds het voorwerp uit van regelgeving in het Belgische recht, krachtens de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, de veiligheidsadviezen en de publiek gereguleerde dienst.
	(2)	Art. 19	"
	(3)	Art. 19	"
Art. 15	(1)	Art. 20, § 1	Melding incidenten
	(2)	Art. 20, § 1, lid 2	

	(3)	Art. 20, § 3	
	(4)	Art. 20, § 4	
Art. 16		-	Lidstaten moedigen het gebruik van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiligings- en weerbaarheidsmaatregelen aan, het betreft geen verplichting waardoor omzetting niet vereist is.
Art. 17	(1)	Art. 14, § 1	
	(2)	Art. 14, § 2	
	(3)	Art. 14, § 3	
	(4)	Art. 14, § 3, lid 1	
Art. 18	(1)	-	Bepaling betreffende het organiseren van adviesmissies door de Europese Commissie die derhalve niet het onderwerp moet uitmaken van een omzetting.
	(2)	-	"
	(3)	-	"
	(4)	Art. 14, § 4, lid 2	
	(5)	-	Bepaling betreffende het organiseren van adviesmissies door de Europese Commissie die derhalve niet het onderwerp moet uitmaken van een omzetting.
	(6)	-	"

	(7)	Art. 14, § 4, lid 1	
	(8)	-	Bepaling betreffende het organiseren van adviesmissies door de Europese Commissie die derhalve niet het onderwerp moet uitmaken van een omzetting.
	(9)	-	"
	(10)	-	"
Art. 19	(1)	-	Bepaling betreffende de oprichting van de Groep voor de Weerbaarheid van kritieke entiteiten, dewelke de Europese Commissie ondersteunt en de samenwerking en informatie-uitwisseling tussen de lidstaten faciliteert, die derhalve niet het onderwerp moet uitmaken van een omzetting.
	(2)	-	"
	(3)	-	"
	(4)	-	"
	(5)	-	"
	(6)	-	"
	(7)	-	"
Art. 20	(1)	-	Bepaling betreffende de ondersteuning die de Europese Commissie kan bieden aan de bevoegde autoriteiten en kritieke entiteiten, die derhalve niet het onderwerp moet uitmaken van een omzetting.
	(2)	-	"

	(3)	-	"
Art. 21	(1)	Art. 33 - 35	
	(2)	Art. 33	
	(3)	Art. 33, lid 2	
	(4)	Art. 34	
	(5)	Art. 34, § 5	
Art. 22		Art. 36 t.e.m. 46	
Art. 23		-	Bepaling betreffende de bevoegdheidsdelegatie die wordt toegekend aan de Europese Commissie dient niet omgezet te worden.
Art. 24		-	Bepaling betreffende de comitéprocedure dient niet omgezet te worden.
Art. 25		-	Bepaling betreffende rapportage door de Europese Commissie dient derhalve niet omgezet te worden.
Art. 26		-	Bepaling betreffende de omzetting van de Richtlijn moet wel geïmplementeerd maar niet omgezet worden.
Art. 27		-	Bepaling betreffende de intrekking van de Richtlijn 2008/114/EG moet derhalve niet omgezet worden.
Art. 28		-	Bepaling betreffende de inwerkingtreding van de richtlijn moet derhalve niet omgezet worden.

Art. 29	-	Bepaling betreffende de adresstaten van de Richtlijn moet derhalve niet omgezet worden.
Bijlage	Bijlage	De bijlage van het ontwerp bevat tevens de bevoegde autoriteiten zoals bedoeld in artikel 9.2 van de Richtlijn.

TABLEAU DE CORRESPONDANCE

DIRECTIVE – PROJET DE LOI

Articles de la directive (UE) 2022/2557 relative à la résilience des entités critiques et abrogeant la directive 2008/114/CE (II)		Articles du projet de loi	Commentaire
Art. 1	(1)	-	La disposition ne doit pas être transposée – l'objet de la directive
	(2)	Art. 6, § 1	
	(3)	Art. 6, § 2	
	(4)	Art. 23	
	(5)	-	
	(6)	Art. 7, § 1	
	(7)	Art. 7, § 2	
	(8)	-	
	(9)	-	
Art. 2	(1)	Art. 3, 3°	
	(2)	Art. 3, 4°	
	(3)	Art. 3, 5°	
	(4)	Art. 3, 6°	

	(5)	Art. 3, 7°	
	(6)	Art. 3, 8°	
	(7)	Art. 3, 9°	
	(8)	-	Cette définition n'est pas transposée car le terme n'est pas utilisé dans le projet de loi. De plus, le terme n'est utilisé qu'à l'article 16 de la directive, qui stipule que, le cas échéant et sans imposer ni favoriser l'utilisation d'un type particulier de technologie, les États membres encouragent l'utilisation des normes et spécifications techniques européennes et internationales pertinentes pour les mesures de sécurité et de résilience applicables aux entités critiques.
	(9)	-	Idem: art. 2, (8)
	(10)	Art. 3, 11°; annexe	
Art. 3		-	La disposition ne doit pas être transposée – il s'agit du principe d'harmonisation minimale de la directive.
Art. 4	(1)	Art. 22, al. 1 et al. 3	
	(2)	Art. 22, al. 4	
	(3)	Art. 21, §2	Rapport de la stratégie à la Commission européenne par les États membres: l'autorité nationale compétente respecte toutes les obligations de rapport prévues par la directive.
Art. 5	(1)	Art. 8, §§ 1 - 3	
	(2)	Art. 8, § 4	

	(3)	Art. 8, § 2	
	(4)	Art. 21, § 2	Rapports à la Commission européenne: l'autorité nationale compétente se conforme à toutes les obligations de rapport prévues par la directive.
	(5)	-	Concerne la possibilité pour la Commission européenne d'établir un modèle de rapport commun volontaire qui ne nécessiterait pas de transposition.
Art. 6	(1)	Art. 12, § 3	
	(2)	Art. 10, § 1; Art. 11, § 1	
	(3)	Art. 13, § 1; Art. 18, § 4	
	(4)	Art. 12, § 4	
	(5)	Art. 12, § 3	
	(6)	-	Cette disposition ne devrait pas être transposée car elle prévoit la possibilité pour la Commission européenne d'émettre des recommandations et des guides non contraignants pour aider les États membres à identifier les entités critiques.
Art. 7	(1)	Art. 11, § 2	
	(2)	Art. 21, § 2	Rapport à la Commission européenne par les États membres après l'identification des entités critiques: l'autorité nationale compétente se conforme à toutes les obligations de rapport prévues par la directive.

	(3)	-	Cette disposition ne doit pas être transposée: la Commission européenne adopte des lignes directrices non contraignantes pour faciliter l'application des critères de l'article 7, paragraphe 1.
Art. 8		Art. 6, § 1	L'article 5, paragraphe 1, prévoit que lorsque des entités critiques des secteurs de la banque, de l'infrastructure des marchés financiers et de l'infrastructure numérique sont tenues de prendre ou ont pris des mesures équivalentes en vertu d'une autre législation, le chapitre 4, section 2, le chapitre 5 et le chapitre 7 ne s'appliquent pas à ces entités critiques.
Art. 9	(1)	Art. 3, 2°; annexe	Les autorités sectorielles sont désignées comme autorité compétente pour les secteurs énumérés dans l'annexe et relevant de leur juridiction.
	(2)	Art. 21, § 1	Est désigné comme le point de contact central national.
	(3)	-	Rapports d'incidents à la Commission européenne: l'autorité nationale compétente se conforme à toutes les obligations en matière de rapports prévues par la directive. En outre, cette disposition prévoit également l'obligation pour la Commission européenne d'élaborer un modèle de rapport commun.
	(4)	-	Cette disposition ne devrait pas être transposée : l'État membre devrait assurer les pouvoirs nécessaires et les ressources financières adéquates pour réaliser effectivement et efficacement les tâches qui leur sont assignées.
	(5)	Art. 25	L'État membre veille à ce que l'autorité compétente consulte les autres autorités nationales concernées et coopère avec elles.
	(6)	Art. 25	

	(7)	-	Cette disposition ne concerne qu'une obligation des États membres envers la Commission européenne et ne devrait donc pas faire l'objet d'une transposition.
	(8)	-	Cette disposition ne doit pas être transposée car elle n'impose qu'une obligation à la Commission européenne.
Art. 10	(1)	Art. 21, § 3	Le rôle de coordination de l'autorité nationale compétente sera précisé dans une décision d'exécution. Ce rôle consiste à faciliter l'échange d'informations et la coopération entre les autorités compétentes et à les aider à s'acquitter des obligations découlant de la présente directive.
	(2)	Art. 21, § 3	
	(3)	Art. 24	
Art. 11	(1)	Art. 15	
	(2)	Art. 15	
Art. 12	(1)	Art. 17, § 1, al. 1	
	(2)	Art. 17, § 1, al. 2 et § 2	
Art. 13	(1)	Art. 18, §§ 1-2	
	(2)	Art. 18, § 4	
	(3)	Art. 16	Cette disposition impose à chaque entité critique de désigner un officier de liaison ou équivalent comme point de contact avec les autorités compétentes. Un point de contact fonctionnant vingt-quatre heures sur vingt-quatre a été choisi. Il appartient à l'entité

			critique d'assurer une permanence garantie par une ou plusieurs personnes habilitées à traiter les questions relatives à la résilience de l'entité critique.
	(4)	-	Cette disposition ne doit pas être transposée car elle n'impose qu'une obligation à la Commission européenne.
	(5)	-	Cette disposition ne doit pas être transposée car elle n'impose qu'une obligation à la Commission européenne.
	(6)	-	Cette disposition ne doit pas être transposée car elle n'impose qu'une obligation à la Commission européenne.
Art. 14	(1)	Art. 19	La vérification de la sécurité visée par cette disposition fait déjà l'objet d'une réglementation en droit belge, en vertu de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé.
	(2)	Art. 19	"
	(3)	Art. 19	"
Art. 15	(1)	Art. 20, § 1	Notification des incidents
	(2)	Art. 20, § 1, al. 2	
	(3)	Art. 20, § 3	
	(4)	Art. 20, § 4	
Art. 16		-	Les États membres encouragent l'utilisation des normes et spécifications techniques européennes et internationales relatives

			aux mesures de sécurité et de résilience; il ne s'agit pas d'une obligation et la transposition n'est donc pas requise.
Art. 17	(1)	Art. 14, § 1	
	(2)	Art. 14, § 2	
	(3)	Art. 14, § 3	
	(4)	Art. 14, § 3, al. 1	
Art. 18	(1)	-	Disposition concernant l'organisation de missions consultatives par la Commission européenne qui ne devrait donc pas faire l'objet d'une transposition.
	(2)	-	"
	(3)	-	"
	(4)	Art. 14, § 4, al. 2	
	(5)	-	Disposition concernant l'organisation de missions consultatives par la Commission européenne qui ne devrait donc pas faire l'objet d'une transposition.
	(6)	-	"
	(7)	Art. 14, § 4, al. 1	
	(8)	-	Disposition concernant l'organisation de missions consultatives par la Commission européenne qui ne devrait donc pas faire l'objet d'une transposition.

	(9)	-	"
	(10)	-	"
Art. 19	(1)	-	La mise en place du Groupe de Résilience des Entités Critiques, que la Commission européenne soutient et qui facilite la coopération et l'échange d'informations entre les États membres, qui ne devrait donc pas faire l'objet d'une transposition.
	(2)	-	"
	(3)	-	"
	(4)	-	"
	(5)	-	"
	(6)	-	"
	(7)	-	"
Art. 20	(1)	-	Disposition relative au soutien que la Commission européenne peut apporter aux autorités compétentes et aux entités critiques, qui ne devrait donc pas faire l'objet d'une transposition.
	(2)	-	"
	(3)	-	"
Art. 21	(1)	Art. 33 - 35	
	(2)	Art. 33	

	(3)	Art. 33, al. 2	
	(4)	Art. 34	
	(5)	Art. 34, § 5	
Art. 22		Art. 36 jusqu'à 46	
Art. 23		-	La disposition relative à la délégation de pouvoirs accordée à la Commission européenne ne doit pas être transposée.
Art. 24		-	La disposition relative à la procédure de comité ne doit pas être transposée.
Art. 25		-	La disposition relative à l'établissement de rapports par la Commission européenne ne doit pas être transposée.
Art. 26		-	Disposition de transposition à mettre en œuvre mais non transposée.
Art. 27		-	Disposition relative à l'abrogation de la directive 2008/114/CE ne doit pas être transposée.
Art. 28		-	La disposition relative à l'entrée en vigueur ne doit pas être transposée.
Art. 29		-	La disposition de la directive relative aux états d'adresse ne doit pas être transposée.
Annexe		Annexe	L'annexe du projet énumère également les autorités compétentes visées à l'article 9, paragraphe 2, de la directive.

CONCORDANTIETABEL

WETSONTWERP – RICHTLIJN

TABLEAU DE CORRESPONDANCE

PROJET DE LOI – DIRECTIVE

Wetsontwerp – Projet de loi	Richtlijn 2022/2557 – Directive 2022/2557
Hoofdstuk 1: Algemene bepalingen – Chapitre 1: Dispositions générales	
Art. 1	Louter nationale wetsbepaling om de grondwettelijke grondslag van de wet te preciseren – Disposition strictement nationale précisant le fondement constitutionnel de la loi
Art. 2	**Art. 26.2**
Hoofdstuk 2: Definities – Chapitre 2: Définitions	
Art. 3, 1°	Louter nationale definitie – Définition strictement nationale
Art. 3, 2°	Louter nationale definitie – Définition strictement nationale
Art. 3, 3°	**Art. 2.1**
Art. 3, 4°	**Art. 2.2**
Art. 3, 5°	**Art. 2.3**
Art. 3, 6°	**Art. 2.4**
Art. 3, 7°	**Art. 2.5**
Art. 3, 8°	**Art. 2.6**
Art. 3, 9°	**Art. 2.7**
Art. 3, 10°	Louter nationale definitie – Définition strictement nationale
Art. 3, 11°	**Art. 2.10**
Art. 3, 12°	Louter nationale definitie – Définition strictement nationale
Art. 3, 13°	Louter nationale definitie – Définition strictement nationale
Hoofdstuk 3: Toepassingsgebied – Chapitre 3: Champ d'application	
Art. 4	Louter nationale definitie – Définition strictement nationale

Art. 5	**Bijlage – Annexe**
Art. 6 § 1	**Art. 8**
Art. 6, § 2	**Art. 1.3**
Art. 7	**Art. 1.6; Art. 1.7**
Hoofdstuk 4: Identificatieprocedure – Chapitre 4: Procédure d'identification	
Afdeling 1: *Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructuren* ***– Section 1re:*** *Identifications et désignation des entités critiques et des infrastructures critiques*	
Art. 8, § 1	**Art. 5.1, lid 1 – al. 1**
Art. 8, § 2	**Art. 5.1, lid 1 – al. 1**
Art. 8, § 3	**Art. 5.1, lid 1 - al. 1**
Art. 8, § 4	**Art. 5.2**
Art. 9, § 1	Louter nationale bepaling – Disposition strictement nationale
Art. 9, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 9, § 3	Louter nationale bepaling – Disposition strictement nationale
Art. 9, § 4	Louter nationale bepaling – Disposition strictement nationale
Art. 10, § 1	Nationale bepaling waarin de identificatieprocedure uit art. 6 en 7 ter verduidelijking wordt opgesomd – Disposition nationale énumérant la procédure d'identification des articles 6 et 7 pour clarification
Art. 10, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 10, § 3	Louter nationale bepaling – Disposition strictement nationale
Art. 10, § 4	**Art. 6.4**
Art. 11, § 1	**Art. 6.2**
Art. 11, § 2	**Art. 7.1**
Art. 12, § 1	**Art. 6.3**

Art. 12, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 12, § 3	**Art. 6.1, art. 6.5**
Art. 12, § 4	**Art. 6.4**
Art. 13, § 1	**Art. 6.3**
Art. 13, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 13, § 3	Louter nationale bepaling – Disposition strictement nationale
Afdeling 2: *Kritieke entiteiten van bijzonder Europees Belang* ***– Section 2:*** *Entités critiques revêtant une importance européenne particulière*	
Art. 14, § 1	**Art. 17.1**
Art. 14, § 2	**Art. 17.2**
Art. 14, § 3	**Art. 17.3**
Art. 14, § 4	**Art. 18.4; art. 18.7**
Art. 15	**Art. 11**
Hoofdstuk 5: Interne weerbaarheidsmaatregelen van de kritieke entiteit – Chapitre 5: Mesures internes de la résilience des entités critiques	
Art. 16	**Art. 13.3**
Art. 17, § 1	**Art. 12.1; Art. 12.2, lid 1 – al. 1**
Art. 17, § 2	**Art. 12.2, lid 2 – al. 2**
Art. 18, § 1	**Art. 13.1; art. 13.2**
Art. 18, § 2	**Art. 13.1**
Art. 18, § 3	**Art. 6.3, lid 2 – al. 2**
Art. 18, § 4	**Art. 13.2**
Art. 18, § 5	Louter nationale bepaling – Disposition strictement nationale
Art. 19	**Art. 14**
Art. 20, § 1	**Art. 15.1; art. 15.2**

Art. 20, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 20, § 3	**Art. 15.3**
Art. 20, § 4	**Art. 15.4**
Hoofdstuk 6: Rapportage en informatie-uitwisseling – Chapitre 6: Rapports et échange d'informations	
Afdeling 1: *De bevoegde autoriteiten* ***– Section 1re:*** *Les autorités compétentes*	
Art. 21, § 1	**Art. 9.1; art. 9.2**
Art. 21, § 2	**Art. 9.1**
Art. 21, § 3	**Art. 9.1**
Art. 22	**Art. 4**
Afdeling 2: *Informatie uitwisseling* ***– Section 2:*** *Échange d'informations*	
Art. 23	**Art. 1.4**
Art. 24	**Art. 10.3**
Art. 25	**Art. 9.6**
Art. 26	Louter nationale bepaling – Disposition strictement nationale
Art. 27	Louter nationale bepaling – Disposition strictement nationale
Art. 28	Louter nationale bepaling – Disposition strictement nationale
Art. 29	**Art. 10.3, art. 1.4, art. 15.3**
Art. 30	Louter nationale bepaling – Disposition strictement nationale
Art. 31	Louter nationale bepaling – Disposition strictement nationale
Art. 32	Louter nationale bepaling – Disposition strictement nationale
Hoofdstuk 7: Controle en sancties – Chapitre 7: Contrôle et sanctions	
Afdeling 1: *Inspecties en audits* ***– Section 1re:*** *Inspections et audits*	

Art. 33	**Art. 21.1, a**) bij delegatie aan de Koning – par délégation au Roi; **Art. 21.2: art. 21.3**
Art. 34, § 1	**Art. 21.1; art. 21.2**
Art. 34, § 2	**Art. 21.1; art. 21.2**
Art. 34, § 3	**Art. 21.4**
Art. 34, § 4	**Art. 21.4**
Art. 34, § 5	Louter nationale bepaling – Disposition strictement nationale
Art. 35	**Art. 21.1, b)** bij delegatie aan de Koning – par délégation au Roi
Afdeling 2: *Procedure van de sancties* ***– Section 2:*** *Procédure de sanctions*	
Art. 36, § 1	Louter nationale bepaling – Disposition strictement nationale
Art. 36, § 2	Louter nationale bepaling – Disposition strictement nationale
Art. 37	**Art. 22**
Art. 38	**Art. 22**
Art. 39	**Art. 22**
Art. 40	Louter nationale bepaling – Disposition strictement nationale
Afdeling 3: *Strafrechtelijke sancties* ***– Section 3:*** *Les sanctions pénales*	
Art. 41, § 1	**Art. 22**
Art. 41, § 2	**Art. 22**
Art. 41, § 3	**Art. 22**
Afdeling 4: *Administratieve sancties* ***– Section 4:*** *Les sanctions administratives*	
Art. 42, § 1	**Art. 22**
Art. 42, § 2	**Art. 22**
Art. 42, § 3	**Art. 22**
Art. 42, § 4	**Art. 22**

Art. 42, § 5	**Art. 22**
Art. 43, § 1	**Art. 22**
Art. 43, § 2	**Art. 22**
Art. 43, § 3	**Art. 22**
Art. 43, § 4	**Art. 22**
Art. 43, § 5	**Art. 22**
Art. 44	**Art. 22**
Art. 45, § 1	**Art. 22**
Art. 45, § 2	**Art. 22**
Art. 45, § 3	**Art. 22**
Art. 46	**Art. 22**
Hoofdstuk 8: Sector Overheid – Chapitre 8: Le secteur des administrations publiques	
Art. 47, § 1	Bijlage, bij delegatie aan de Koning – Annexe, par délégation au Roi
Art. 47, § 2	Louter nationale bepaling – Disposition strictement nationale
Hoofdstuk 9: Diverse bepalingen – Chapitre 9: Dispositions diverses	
***Afdeling 1**: Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie – **Section 1re**: Modifications de la loi du 13 juin 2005 relative aux communications électronique*	
Art. 48	Louter nationale bepaling – Disposition strictement nationale
Art. 49	Louter nationale bepaling – Disposition strictement nationale
Art. 50	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 2**: Wijziging van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit – **Section 2**: Modification de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l'information et la communication et désignant une autorité nationale de certification de cybersécurité*	
Art. 51	Louter nationale bepaling – Disposition strictement nationale

Art. 52	Louter nationale bepaling – Disposition strictement nationale
Art. 53	Louter nationale bepaling – Disposition strictement nationale
Art. 54	Louter nationale bepaling – Disposition strictement nationale
Art. 55	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 3**: Wijziging van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector – **Section 3**: Modification de la loi du 17 janvier 2003 relative au status du régulateur du secteur belge des postes et télécommunications*	
Art. 56	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 4:** Wijziging van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België – **Section 4:** Modification de la loi du 22 février 1998 portant le statut organique de la Banque nationale de Belgique*	
Art. 57	Louter nationale bepaling – Disposition strictement nationale
Art. 58	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 5**: Wijziging van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen – **Section 5**: Modification de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations*	
Art. 59	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 6**: Wijziging van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt – **Section 6:** Modification de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité*	
Art. 60	Louter nationale bepaling – Disposition strictement nationale
***Afdeling 7**: wijziging van het Strafwetboek – **Section 7**: Modification du Code pénal*	
Art. 61	Louter nationale bepaling – Disposition strictement nationale
Art. 62	Louter nationale bepaling – Disposition strictement nationale

Afdeling 8: *Wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren betreffende het Federaal Agentschap voor Nucleaire Controle –* ***Section 8:*** *Modification de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Controle nucléaire*	
Art. 63	Louter nationale bepaling – Disposition strictement nationale
Afdeling 9. *Wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging –* ***Section 9.*** *Modification de la loi du 10 juillet 2006 relative à l'analyse de la menace*	
Art. 64	Louter nationale bepaling – Disposition strictement nationale
Afdeling 10. *Wijziging van de wet van […] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid –* ***Section 10.*** *Modification de la loi […] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*	
Art. 65	Louter nationale bepaling – Disposition strictement nationale
Art. 66	Louter nationale bepaling – Disposition strictement nationale
Art. 67	Louter nationale bepaling – Disposition strictement nationale
Art. 68	Louter nationale bepaling – Disposition strictement nationale
Art. 69	Louter nationale bepaling – Disposition strictement nationale
Art. 70	Louter nationale bepaling – Disposition strictement nationale
Art. 71	Louter nationale bepaling – Disposition strictement nationale
Art. 72	Louter nationale bepaling – Disposition strictement nationale
Art. 73	Louter nationale bepaling – Disposition strictement nationale
Art. 74	Louter nationale bepaling – Disposition strictement nationale
Art. 75	Louter nationale bepaling – Disposition strictement nationale

Art. 76	Louter nationale bepaling – Disposition strictement nationale
Hoofdstuk 10: Slotbepalingen – Chapitre 10: Dispositions finales	
Art. 77	Louter nationale bepaling – Disposition strictement nationale
Art. 78	Louter nationale bepaling – Disposition strictement nationale
Art. 79	Louter nationale bepaling – Disposition strictement nationale
Art. 80	Louter nationale bepaling – Disposition strictement nationale
Art. 81	Louter nationale bepaling – Disposition strictement nationale
Bijlage – Annexe	**Bijlage – Annexe**

COÖRDINATIE VAN DE ARTIKELEN

Basistekst	**Tekst aangepast aan het wetsontwerp**
Wet van 13 juni 2005 betreffende de elektronische communicatie	
Art. 28/3	Art. 28/3
§ 1. Elke onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, willigt op schriftelijk verzoek van een andere onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, de redelijke verzoeken om toegang tot zijn passieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische-communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een precies tijdschema.	§ 1. Elke onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, willigt op schriftelijk verzoek van een andere onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, de redelijke verzoeken om toegang tot zijn passieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische-communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een precies tijdschema.
§ 2. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:	§ 2. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:
1° de technische geschiktheid van de passieve infrastructuur waarvoor om toegang wordt verzocht voor het onderbrengen van de in paragraaf 1 bedoelde elementen van elektronische-communicatienetwerken met hoge snelheid;	1° de technische geschiktheid van de passieve infrastructuur waarvoor om toegang wordt verzocht voor het onderbrengen van de in paragraaf 1 bedoelde elementen van elektronische-communicatienetwerken met hoge snelheid;
2° de beschikbaarheid van ruimte om de in paragraaf 1 bedoelde elementen van elektronische-communicatienetwerken met hoge snelheid te huisvesten, met inbegrip van de toekomstige behoefte aan ruimte van de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, voor zover die afdoende aangetoond zijn;	2° de beschikbaarheid van ruimte om de in paragraaf 1 bedoelde elementen van elektronische-communicatienetwerken met hoge snelheid te huisvesten, met inbegrip van de toekomstige behoefte aan ruimte van de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, voor zover die afdoende aangetoond zijn;
3° overwegingen met betrekking tot veiligheid en volksgezondheid;	3° overwegingen met betrekking tot veiligheid en volksgezondheid;
4° de integriteit en veiligheid van de passieve infrastructuur, met name van kritieke nationale infrastructuur bedoeld in de wet van 1 juli 2011	4° de integriteit en veiligheid van de passieve infrastructuur, met name van kritieke nationale infrastructuur bedoeld in **de wet van …**

betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	**betreffende de weerbaarheid van kritieke entiteiten**;
5° het risico van ernstige verstoring tussen de geplande elektronische-communicatiediensten en de diensten die via de passieve infrastructuur worden verstrekt;	5° het risico van ernstige verstoring tussen de geplande elektronische-communicatiediensten en de diensten die via de passieve infrastructuur worden verstrekt;
6° de vraag of de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is beschikt over levensvatbare alternatieve middelen voor het verlenen van fysieke wholesaletoegang tot de passieve infrastructuur die geschikt zijn voor het aanbieden van elektronische-communicatienetwerken met hoge snelheid, op voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.	6° de vraag of de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is beschikt over levensvatbare alternatieve middelen voor het verlenen van fysieke wholesaletoegang tot de passieve infrastructuur die geschikt zijn voor het aanbieden van elektronische-communicatienetwerken met hoge snelheid, op voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.
Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is de redenen voor de weigering op.	Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is de redenen voor de weigering op.
§ 3. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar het Instituut, overeenkomstig artikel 4 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.	§ 3. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar het Instituut, overeenkomstig artikel 4 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.
§ 4. Dit artikel laat het eigendomsrecht van de eigenaar van de passieve infrastructuur, indien de beheerder van de passieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, om de toelatingen en vergunningen te bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn	§ 4. Dit artikel laat het eigendomsrecht van de eigenaar van de passieve infrastructuur, indien de beheerder van de passieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare elektronische-communicatienetwerken aanbiedt of daartoe gemachtigd is, om de toelatingen en vergunningen te bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn

elektronische-communicatienetwerk met hoge snelheid, onverlet.	elektronische-communicatienetwerk met hoge snelheid, onverlet.
Art. 105	Art. 105
§ 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid, 1°, alvorens een element van hun 5G-netwerk te gebruiken.	§ 1. Om de belangen te vrijwaren waarvan sprake in artikel 3, § 1, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moeten de MNO's een machtiging krijgen die gezamenlijk is opgesteld door de betrokken ministers beoogd in het derde lid, 1°, alvorens een element van hun 5G-netwerk te gebruiken.
Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO's diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.	Rekening houdende met de in het eerste lid bedoelde belangen en bij besluit vastgesteld na overleg in de Ministerraad, kan de Koning bepalen dat deze machtiging ook noodzakelijk is voordat de MNO's diensten van aanbieders kunnen genieten die erin bestaan gericht tussenbeide te komen in het beheer van dat netwerk, met name in geval van een incident of grote wijziging van het netwerk, of dagelijks elementen van het netwerk te beheren of te superviseren, of ook noodzakelijk is voordat ze bepaalde van deze diensten kunnen genieten.
Voor de toepassing van dit artikel wordt verstaan onder:	Voor de toepassing van dit artikel wordt verstaan onder:
1° betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken;	1° betrokken ministers: de Eerste minister, de minister van Telecommunicatie, de minister van Defensie, de minister van Justitie, de minister van Binnenlandse Zaken en de minister van Buitenlandse Zaken;
2° 5G-netwerk: een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.	2° 5G-netwerk: een elektronische-communicatienetwerk waarvan het radiotoegangsnetwerk gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie.
Het eerste en het tweede lid zijn niet van toepassing:	Het eerste en het tweede lid zijn niet van toepassing:
1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;	1° voor het gebruik van passieve elementen van het netwerk, namelijk elementen die niet door een energiebron worden gevoed;

2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;	2° voor de netwerkaansluitpunten voor zover ze geen radiogedeelte bevatten dat gebaseerd is op een radio-interface die gespecificeerd is in de ITU-R-aanbeveling M.2150 van de Internationale Telecommunicatie Unie;
3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.	3° voor de elementen van mobiele netwerken van de vierde generatie en vroegere generaties, op voorwaarde dat ze niet noodzakelijk zijn voor het aanbieden van een 5G-netwerk.
Indien het gebruik van het netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.	Indien het gebruik van het netwerkelement of het beroep op de dienstenaanbieder reeds bestaat op de datum van inwerkingtreding van het koninklijk besluit bedoeld in paragraaf 4, eerste lid, wordt een machtiging tot regularisatie gevraagd in de twee maanden die volgen op die datum.
§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:	§ 2. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, kan de Koning, bij een besluit vastgesteld na overleg in de Ministerraad:
1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;	1° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar één of meer categorieën van MVNO's;
2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht ASTRID en naar de exploitanten van een privaat elektronische-communicatienetwerk die aangewezen zijn als exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	2° de verplichting om de machtigingen bedoeld in paragraaf 1 te krijgen, uitbreiden naar de naamloze vennootschap van publiek recht ASTRID en naar de exploitanten van een privaat elektronische-communicatienetwerk die aangewezen zijn als **kritieke entiteit in de zin van de wet van … betreffende de weerbaarheid van kritieke entiteiten;**
3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere exploitanten van een privaat elektronische-communicatienetwerk aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;	3° een of meer autoriteiten opdragen om via individuele beslissing, wanneer dat noodzakelijk is om de in paragraaf 1, eerste lid bedoelde belangen te vrijwaren, de andere exploitanten van een privaat elektronische-communicatienetwerk aan te wijzen die onderworpen zijn aan de verplichting om de in paragraaf 1 bedoelde machtigingen te krijgen;
4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;	4° de hypothesen preciseren waarin een machtiging zoals bedoeld in paragraaf 1, eerste lid, noodzakelijk is in geval van een update van software of hardware van het netwerk;

§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.	§ 3. De verzoeker dient zijn dossier in bij het Instituut, volgens de nadere regels die het op zijn website bepaalt.
De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.	De Koning stelt, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels voor de behandeling van het verzoek en de samenstelling van het dossier vast.
De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.	De betrokken ministers, het Instituut en de inlichtingen- en veiligheidsdiensten kunnen informatie of aanvullende documenten vragen aan de verzoeker of aan iedere persoon die op nuttige wijze kan bijdragen tot hun informatie.
§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element dat hun beslissing ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.	§ 4. Wanneer ze hun beslissing nemen na het onderzoek van het in paragraaf 1 bedoelde verzoek of deze op eigen initiatief herzien wegens een nieuw element dat hun beslissing ter discussie stelt, leggen de betrokken ministers de beperkingen en toepassingstermijnen ten uitvoer die vastgesteld zijn door de Koning, bij een besluit vastgesteld na overleg in de Ministerraad, betreffende het gebruik, op het nationale grondgebied of in de gevoelige zones van dit grondgebied, van netwerkelementen of van diensten van leveranciers die een hoog risico vormen.
Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.	Die beperkingen en toepassingstermijnen mogen enkel vastgesteld worden om de bescherming van de belangen bedoeld in paragraaf 1, eerste lid, te garanderen.
Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.	Wanneer ze op eigen initiatief hun beslissing herzien en wanneer dat gerechtvaardigd is, leggen de betrokken ministers een datum van uitvoering van de nieuwe beslissing vast die later komt dan de termijnen die vastgesteld zijn bij het in het eerste lid bedoelde koninklijk besluit en die minstens vijf jaar na de datum van de kennisgeving ervan valt.
Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:	Het risicoprofiel van een leverancier wordt beoordeeld op basis van de volgende criteria:
1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich	1° de kans dat hij inmenging ondervindt vanwege een land dat geen lidstaat is van de Europese Unie, waarbij een dergelijke inmenging gefaciliteerd kan worden, zonder zich

daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:	daartoe te beperken, door de aanwezigheid van één of meer van de volgende factoren:
a) een sterke link met de overheidsinstanties van het land in kwestie;	a) een sterke link met de overheidsinstanties van het land in kwestie;
b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;	b) de wetgeving van of de situatie in het land in kwestie, met name wanneer er geen democratische of wetgevende controle voorhanden is of bij afwezigheid van overeenkomsten over gegevensbescherming of beveiliging tussen de Europese Unie en het land in kwestie;
c) de karakteristieken van de eigendom van de onderneming van de leverancier;	c) de karakteristieken van de eigendom van de onderneming van de leverancier;
d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;	d) het vermogen van het land in kwestie om enige vorm van pressie uit te oefenen, inclusief wat betreft de plaats van vervaardiging van de apparatuur;
e) het feit dat het land waaruit de leverancier afkomstig is, een offensief cyberbeleid voert of daarbij betrokken is;	e) het feit dat het land waaruit de leverancier afkomstig is, een offensief cyberbeleid voert of daarbij betrokken is;
2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;	2° het vermogen van de leverancier om de bevoorrading te garanderen in termen van tijd en hoeveelheid;
3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging.	3° de algemene kwaliteit van de producten of diensten en de praktijken inzake beveiliging van de leverancier, met inbegrip van de mate van controle over zijn eigen bevoorradingsketen en de vraag of een gepaste hiërarchische indeling van de prioriteiten wordt gegeven aan de praktijken inzake beveiliging
De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen.	De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de in het vierde lid beoogde criteria aanvullen
Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend.	Slechts één van deze criteria kan reeds rechtvaardigen dat een aanbieder wordt aangeduid als een hoog risico vormend
Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.	Het risicoprofiel van een leverancier wordt geëvalueerd op basis van een advies van de inlichtingen- en veiligheidsdiensten voor wat betreft het criterium vastgesteld in het vierde lid, 1°, en op basis van een advies van het Instituut voor wat betreft de criteria vastgesteld in het vierde lid, 2° en 3°.

De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.	De gevoelige zones worden geïdentificeerd door de Koning, op basis van een advies van de Nationale Veiligheidsraad en dit rekening houdend met de aanwezigheid in deze zones van sites gelieerd aan de belangen bedoeld in paragraaf 1, eerste lid.
Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het Belgisch Staatsblad	Het koninklijk besluit dat de gevoelige zones identificeert, wordt bekendgemaakt via vermelding in het Belgisch Staatsblad.
§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.	§ 5. Wanneer de betrokken ministers van plan zijn de machtiging te weigeren, daar voorwaarden aan te koppelen of hun beslissing te herzien, beschikt de verzoeker, na de ontwerpbeslissing te hebben ontvangen, over achtentwintig dagen tijd om zijn schriftelijke opmerkingen voor te leggen.
De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.	De verzoeker wordt de kans geboden om te worden gehoord. Hij mag zich laten vergezellen door de technische of juridische raadgevers van zijn keuze.
De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.	De betrokken ministers kunnen zich laten vertegenwoordigen door het bestuur van hun keuze. Het Instituut en de inlichtingen- en veiligheidsdiensten kunnen aan de hoorzitting deelnemen.
§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.	§ 6. De betrokken ministers nemen samen één beslissing. Het Instituut stelt alle nuttige daden met het oog op de voorbereiding ervan.
Binnen de door de Koning vastgestelde termijn, die ingaat vanaf de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.	Binnen de door de Koning vastgestelde termijn, die ingaat vanaf de indiening van het verzoek, ontvangt de verzoeker ofwel de beslissing van de ministers waarin de machtiging wordt verleend, ofwel de ontwerpbeslissing waarin ze de machtiging weigeren of voorwaarden daaraan koppelen.
In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen.	In geval van een hoorzitting of van schriftelijke opmerkingen van de verzoeker, waarvan sprake in paragraaf 5, nemen de ministers hun beslissing uiterlijk binnen de termijn die door de Koning is vastgesteld en die ingaat vanaf de ontvangst van de schriftelijke opmerkingen of vanaf de datum van de hoorzitting, waarbij de datum die het laatst komt in aanmerking wordt genomen

Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, derde lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.	Het verzoek om inlichtingen of om documenten, waarvan sprake in paragraaf 3, derde lid, of dat gericht is aan de verzoeker om zijn dossier te vervolledigen, schorst de termijnen die vastgesteld zijn in het tweede en het derde lid, tot de dag waarop de gevraagde inlichtingen of documenten worden verstrekt.
Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.	Het uitblijven van een beslissing of ontwerpbeslissing bedoeld in het tweede lid binnen de krachtens het tweede of het derde lid vastgestelde termijn staat gelijk aan een weigering.
§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.	§ 7. De persoon die een kopie krijgt van de in paragraaf 4, achtste lid, bedoelde lijst van de gevoelige zones, mag die maar verzenden aan de personen die daar kennis van moeten hebben en die daar toegang toe moeten hebben om hun functies of opdracht in het kader van de uitrol en de exploitatie van het 5G-netwerk uit te voeren.
Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100 000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.	Wordt bestraft met een strafrechtelijke boete van 1000 euro tot 100 000 euro: de persoon die informatie onthult in verband met de in het eerste lid bedoelde lijst aan een persoon die in dat lid niet is beoogd.
Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.	Personen die een verzoek om machtiging of de herziening van een vroegere beslissing behandelen, mogen aan openbare besturen die zij in dat kader raadplegen vertrouwelijke informatie meedelen wanneer dat nodig is voor het vervullen van de taak die zij aan hen toevertrouwen.
De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.	De in het derde lid bedoelde personen en openbare besturen mogen derden geen vertrouwelijke informatie meedelen waarvan zij kennis hebben in het kader van de toepassing van dit artikel, buiten de in de wet bepaalde uitzonderingen.
Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.	Deze vertrouwelijke informatie is die welke als zodanig wordt aangeduid door de persoon die ze heeft verstrekt, onverminderd artikel 23, paragraaf 3, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.
De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn	De schending van het in het vierde lid bedoelde verbod wordt bestraft met de straffen die zijn

bepaald in artikel 458 van het Strafwetboek of met één van die straffen.	bepaald in artikel 458 van het Strafwetboek of met één van die straffen.
§ 8. Wanneer een MNO in België elektronische-communicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuren van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.	§ 8. Wanneer een MNO in België elektronische-communicatiediensten aanbiedt met behulp van een 5G-netwerk, moeten de infrastructuren van dat netwerk zich bevinden op het grondgebied van de lidstaten van de Europese Unie. Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de eisen vaststellen die uit die verplichting voortvloeien.
Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.	Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, legt de Koning de in het eerste lid bedoelde MNO's de noodzakelijke regels op opdat zij de activiteiten die absoluut noodzakelijk zijn voor de werking, de veiligheid en de continuïteit van hun netwerk, die Hij bepaalt, uitoefenen binnen het grondgebied van de lidstaten van de Europese Unie.
Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en exploitanten van een privaat elektronische-communicatienetwerk die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.	Rekening houdende met de belangen bedoeld in paragraaf 1, eerste lid, en bij een besluit vastgesteld na overleg in de Ministerraad, kan de Koning de regels en eisen bedoeld in het eerste en tweede lid uitbreiden naar de MVNO's en exploitanten van een privaat elektronische-communicatienetwerk die onderworpen zijn aan de machtigingen bedoeld in paragraaf 1.
Art. 126/3	Art. 126/3
§ 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:	§ 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit:
- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;	- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;
- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren,	- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren,

en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.	en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.
In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:	In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:
a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.	a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.
In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:	In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2:
a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.	a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren; c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.	Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.
De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.	De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.
De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.	De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.
De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.	De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.
De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.	De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.
De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.	De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.
Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de	Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de

politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.	politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.
Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.	Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.
§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.	§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.
Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.	Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.
De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.	De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:	§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name:
a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;	a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;
b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;	b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;
c) de metro- en de pre-metrostations;	c) de metro- en de pre-metrostations;
d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;	d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;
e) de gebouwen bestemd voor de administratie van douane en accijnzen;	e) de gebouwen bestemd voor de administratie van douane en accijnzen;
f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;	f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, c), van de wet van 5 mei 2014 betreffende de internering;
g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;	g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;	h) de inrichtingen bedoeld in artikel 3.1.a), van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;
i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;	i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;
j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;	j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in **de wet van de wet van … betreffende de weerbaarheid van kritieke entiteiten** en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;
k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;	k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;
l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van diensten van essentiële entiteiten in de zin van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;	l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van diensten van essentiële entiteiten in de zin van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;
m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of	m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of

voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.	voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.
§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:	§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen:
a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;	a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;
b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;	b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;
c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;	c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;
d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:	d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties:
i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;	i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;
ii) de gemeentehuizen en de stadhuizen;	ii) de gemeentehuizen en de stadhuizen;
iii) het koninklijk paleis;	iii) het koninklijk paleis;
iv) de koninklijke domeinen;	iv) de koninklijke domeinen;
v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;	v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;
vi) de gemeenten waar zich militaire domeinen bevinden;	vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;	vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;
e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;	e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;
f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:	f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid:
i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;	i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;
ii) de Nationale Bank van België;	ii) de Nationale Bank van België;
g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.	g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.
§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:	§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen:
a) de ambassades en diplomatieke vertegenwoordigingen;	a) de ambassades en diplomatieke vertegenwoordigingen;
b) de gebouwen bestemd voor de Europese Unie;	b) de gebouwen bestemd voor de Europese Unie;
c) de gebouwen en de infrastructuren bestemd voor de NAVO;	c) de gebouwen en de infrastructuren bestemd voor de NAVO;
d) de instellingen van de Europese Economische Ruimte;	d) de instellingen van de Europese Economische Ruimte;
e) de instellingen van de Verenigde Naties;	e) de instellingen van de Verenigde Naties;
f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.	f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.	§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.
Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.	Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.
Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.	Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.
Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.	Met uitzondering van de in paragraaf 4, b), bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.
Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.	Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.
Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.	Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.
Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.	Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.	Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.
Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.	Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

Art. 3	Art. 3
§ 1. Deze wet is van toepassing op de vrijwillige Europese certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen zoals bedoeld in de Cyberbeveiligingsverordening.	§ 1. Deze wet is van toepassing op de vrijwillige Europese certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen zoals bedoeld in de Cyberbeveiligingsverordening.
§ 2. De hoofdstukken 1 tot 4, 7 en 8, alsook de artikelen 21 en 22, zijn ook van toepassing op een verplichte Europese cyberbeveiligingscertificering.	§ 2. De hoofdstukken 1 tot 4, 7 en 8, alsook de artikelen 21 en 22, zijn ook van toepassing op een verplichte Europese cyberbeveiligingscertificering.
Bij de uitvoering van artikel 21 en 22 in het kader van de in het eerste lid bedoelde certificering zijn artikel 19 en 26 van toepassing.	Bij de uitvoering van artikel 21 en 22 in het kader van de in het eerste lid bedoelde certificering zijn artikel 19 en 26 van toepassing.
De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de hoofdstukken 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van de in het eerste lid bedoelde certificering.	De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, de hoofdstukken 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van de in het eerste lid bedoelde certificering.
§ 3. Deze wet doet geen afbreuk aan de bevoegdheden om een cyberbeveiligingscertificering op te leggen en er toezicht op uit te oefenen waarover de overheden beschikken, met name de markttoezichtautoriteiten of de sectorale overheden bedoeld in artikel 6, 2°, van de wet	§ 3. Deze wet doet geen afbreuk aan de bevoegdheden om een cyberbeveiligingscertificering op te leggen en er toezicht op uit te oefenen waarover de overheden beschikken, met name de markttoezichtautoriteiten of de sectorale overheden bedoeld **in artikel 3, 2°, van de wet**

van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, in artikel 3, 3°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 2, eerste lid, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.	**van … betreffende de weerbaarheid van kritieke entiteiten.**
Met inachtneming van paragraaf 2 zorgen de in het eerste lid bedoelde overheden en de bevoegde inspectiediensten voor het toezicht op en de sancties met betrekking tot verplichte Europese cyberbeveiligingscertificeringen.	Met inachtneming van paragraaf 2 zorgen de in het eerste lid bedoelde overheden en de bevoegde inspectiediensten voor het toezicht op en de sancties met betrekking tot verplichte Europese cyberbeveiligingscertificeringen.
§ 4. Artikel 5, §§ 2 tot 4, is niet van toepassing op de Nationale Bank van België bedoeld in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, noch op de FSMA bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten noch op de FOD Economie bedoeld in het Wetboek van economisch recht.	§ 4. Artikel 5, §§ 2 tot 4, is niet van toepassing op de Nationale Bank van België bedoeld in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, noch op de FSMA bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten noch op de FOD Economie bedoeld in het Wetboek van economisch recht.
§ 5. Deze wet doet geen afbreuk aan de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.	§ 5. Deze wet doet geen afbreuk aan de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.
Art. 6	Art. 6
§ 1. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, voeren hun taken uit in overleg met de overheden, met name met de nationale accreditatieautoriteit. Naargelang het specifieke voorwerp van de certificeringsregeling kunnen de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, ook de private actoren raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.	§ 1. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, voeren hun taken uit in overleg met de overheden, met name met de nationale accreditatieautoriteit. Naargelang het specifieke voorwerp van de certificeringsregeling kunnen de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, ook de private actoren raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.
§ 2. Overeenkomstig artikel 58, lid 7, onder h), van de Cyberbeveiligingsverordening wordt informatie uitgewisseld tussen, enerzijds, de	§ 2. Overeenkomstig artikel 58, lid 7, onder h), van de Cyberbeveiligingsverordening wordt informatie uitgewisseld tussen, enerzijds, de

autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen en, anderzijds, de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of in artikel 7, § § 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, het Belgisch Instituut voor postdiensten en telecommunicatie en de nationale accreditatieautoriteit. Deze informatie is noodzakelijk voor de toepassing van de Cyberbeveiligingsverordening, deze wet of de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. Indien een informatie-uitwisseling persoonsgegevens betreft, gebeurt deze overeenkomstig de bepalingen van hoofdstuk 8. De nadere regels van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.	autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen en, anderzijds, de sectorale overheden en de inspectiediensten, respectievelijk bedoeld **in de artikelen 3, 2°, en 33, van de wet van … betreffende de weerbaarheid van kritieke entiteiten** of in artikel **15, § 2, van de wet van … tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**, het Belgisch Instituut voor postdiensten en telecommunicatie en de nationale accreditatieautoriteit. Deze informatie is noodzakelijk voor de toepassing van de Cyberbeveiligingsverordening, deze wet of de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. Indien een informatie-uitwisseling persoonsgegevens betreft, gebeurt deze overeenkomstig de bepalingen van hoofdstuk 8. De nadere regels van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.
§ 3. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen verstrekken de ontvangers, namelijk een sectorale overheid, een inspectiedienst, de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, § § 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid of in de artikelen 2, eerste lid, 1° en 9°, en 15, § § 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, alle informatie verkregen in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet of een Europese cyberbeveiligingscertificeringsregeling, indien	§ 3. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen verstrekken de ontvangers, namelijk een sectorale overheid, een inspectiedienst, de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, respectievelijk bedoeld in de **artikelen 3, 2°, en 33, van de wet van … betreffende de weerbaarheid van kritieke entiteiten**, in artikel **15, § 2, van de wet van … tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**, alle informatie verkregen in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet of een Europese cyberbeveiligingscertificeringsregeling, indien deze informatie betrekking heeft op een inbreuk op artikel 13 van de voormelde wet van 1 juli 2011, **artikel 30 van de voormelde wet van 26 april 2024**, artikel 11 van het voormelde koninklijk besluit van 2 december 2011 of de

deze informatie betrekking heeft op een inbreuk op artikel 13 van de voormelde wet van 1 juli 2011, de artikelen 20, 21, § 1, en 33, van de voormelde wet van 7 april 2019, artikel 11 van het voormelde koninklijk besluit van 2 december 2011 of de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, en de entiteit waarop de informatie betrekking heeft onder het toezicht staat van voornoemde ontvangers.	afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, en de entiteit waarop de informatie betrekking heeft onder het toezicht staat van voornoemde ontvangers.
§ 4. In het kader van de samenwerking bedoeld in de paragrafen 2 en 3 mogen overheden die uit hoofde van hun staat kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, of aan de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.	§ 4. In het kader van de samenwerking bedoeld in de paragrafen 2 en 3 mogen overheden die uit hoofde van hun staat kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, of aan de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen, indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.
Enkel de noodzakelijke informatie met betrekking tot toezicht, sancties en klachten mogen bekendgemaakt worden. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing. De nadere regels van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.	Enkel de noodzakelijke informatie met betrekking tot toezicht, sancties en klachten mogen bekendgemaakt worden. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing. De nadere regels van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.
Art. 16	Art. 16
§ 1. Na afloop van de inspecties stelt de inspectiedienst een verslag op waarvan een kopie wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen.	§ 1. Na afloop van de inspecties stelt de inspectiedienst een verslag op waarvan een kopie wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen.
§ 2. De verslagen opgesteld door de inspectiedienst mogen geen persoonsgegevens bevatten van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch persoonsgegevens die deze klanten verwerken.	§ 2. De verslagen opgesteld door de inspectiedienst mogen geen persoonsgegevens bevatten van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch persoonsgegevens die deze klanten verwerken.

§ 3. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, in de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, kan de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie krijgen van het in paragraaf 1 bedoelde verslag.	§ 3. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, in de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, kan de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie krijgen van het in paragraaf 1 bedoelde verslag.
In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het verslag bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover:	In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het verslag bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover:
1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;	1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;
2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;	2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;
3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;	3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;
4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.	4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.
§ 4. Met inachtneming van de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging	§ 4. Met inachtneming van **artikel 17 van de wet van … betreffende de weerbaarheid van kritieke entiteiten**, bezorgt de autoriteit

van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het verslag bedoeld in paragraaf 1 aan de sectorale overheid en de inspectiedienst, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011 en in artikel 7, § § 3 en 5, van de voormelde wet van 7 april 2019, die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12° tot 14°, van de Cyberbeveiligingsverordening, indien dit verslag betrekking heeft op een controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in de voormelde wet van 1 juli 2011 of de voormelde wet van 7 april 2019.	bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het verslag bedoeld in paragraaf 1 aan de sectorale overheid en de inspectiedienst, respectievelijk bedoeld in **de artikelen de artikelen 3, 2° en 33, van de voormelde wet van …,** die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12° tot 14°, van de Cyberbeveiligingsverordening, indien dit verslag betrekking heeft op een controle bij een **kritieke entiteit**, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in de voormelde **wet van ….**
Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het verslag bedoeld in paragraaf 1 aan de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, §§ 1 tot 3, van het voormelde koninklijk besluit van 2 december 2011, indien dit verslag betrekking heeft op een controle bij een kritieke infrastructuur als bedoeld in dit koninklijk besluit.	Met inachtneming de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het verslag bedoeld in paragraaf 1 aan de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, indien dit verslag betrekking heeft op een controle bij een **kritieke entiteit als bedoeld in de wet van … betreffende de weerbaarheid van kritieke entiteiten.**
In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de	In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de

doorgifte van het in deze paragraaf bedoelde verslag niet worden geformaliseerd aan de hand van een protocol voor zover:	doorgifte van het in deze paragraaf bedoelde verslag niet worden geformaliseerd aan de hand van een protocol voor zover:
1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;	1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;
2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer;	2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van **de wet van … betreffende de weerbaarheid van kritieke entiteiten**, de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;
3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;	3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;
4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.	4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.
Art. 17	Art. 17
§ 1. De beëdigde leden van de inspectiedienst stellen de in artikel 20, § 1, bedoelde processen-verbaal op.	§ 1. De beëdigde leden van de inspectiedienst stellen de in artikel 20, § 1, bedoelde processen-verbaal op.
§ 2. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 en in de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, krijgt de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie van het proces-verbaal en van alle bijkomende informatie in	§ 2. Op hun verzoek en voor zover dit nodig is voor het vervullen van de opdrachten bedoeld in artikel VIII.30, § 2, van het Wetboek van economisch recht, in hoofdstuk II van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 en in de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie, krijgt de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie van het proces-verbaal en van alle bijkomende informatie in

verband met een controle uitgevoerd door de autoriteit bedoeld in artikel 5, § 1, of door de overheid die door de Koning is aangewezen krachtens artikel 5, § 2.	verband met een controle uitgevoerd door de autoriteit bedoeld in artikel 5, § 1, of door de overheid die door de Koning is aangewezen krachtens artikel 5, § 2.
In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het proces-verbaal bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover:	In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het proces-verbaal bedoeld in het eerste lid niet worden geformaliseerd aan de hand van een protocol voor zover:
1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;	1° de doorgifte noodzakelijk is voor de uitvoering van het eerste lid;
2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;	2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet, van de artikelen 58, lid 7, onder c), en 60, leden 1 en 4, van de Cyberbeveiligingsverordening of van de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie;
3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;	3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;
4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.	4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.
§ 3. Met inachtneming van artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, de bevoegde sectorale overheid en de bevoegde inspectiedienst, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011 en in artikel 7, §§ 3 en 5, van de voormelde wet van 7 april 2019, naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van	§ 3. Met inachtneming van **artikel 18 van de wet van … betreffende de weerbaarheid van kritieke entiteiten,** bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, de bevoegde sectorale overheid en de bevoegde inspectiedienst, respectievelijk bedoeld in de **artikelen 3, 2° en 33, van de voormelde wet van …,** naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening, een volledige kopie van het proces-verbaal en van alle bijkomende informatie in verband met een controle bij een **kritieke entiteit** als bedoeld in de voormelde **wet van ….**

de Cyberbeveiligingsverordening, een volledige kopie van het proces-verbaal en van alle bijkomende informatie in verband met een controle bij een kritieke infrastructuur, aanbieder van essentiële diensten of digitaledienstverlener als bedoeld in de voormelde wet van 1 juli 2011 of de voormelde wet van 7 april 2019.	
Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het proces-verbaal en van alle bijkomende informatie in verband met een controle bij een kritieke infrastructuur, als bedoeld in artikel 2, 3°, van het voormelde koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, aan de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services, als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, §§ 1 tot 3, van dit koninklijk besluit.	Met inachtneming van de afdelingen 1.7 en 11.2.8 van Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, bezorgt de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een kopie van het proces-verbaal en van alle bijkomende informatie in verband met een controle bij een **kritieke entiteit, zoals bedoeld in artikel 3, 3° van de wet van … betreffende de weerbaarheid van kritieke entiteiten,** aan de luchthaveninspectie, de luchtvaartinspectie of de Belgian Supervising Authority for Air Navigation Services.
In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het in deze paragraaf bedoelde proces-verbaal niet worden geformaliseerd aan de hand van een protocol voor zover:	In afwijking van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moet de doorgifte van het in deze paragraaf bedoelde proces-verbaal niet worden geformaliseerd aan de hand van een protocol voor zover:
1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;	1° de doorgifte noodzakelijk is voor de uitvoering van het tweede lid;
2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging	2° de autoriteit die de gegevens ontvangt, deze verwerkt met inachtneming van de bepalingen van **de wet van … betreffende de weerbaarheid van kritieke entiteiten;**

van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer;	
3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;	3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, een voornaam, een particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;
4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.	4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.
Art. 36	Art. 36
§ 1. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:	§ 1. De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:
1° de afgifte van Europese cyberbeveiligingscertificaten en het klachtenbeheer in dit verband door de autoriteit bedoeld in artikel 5, § 1;	1° de afgifte van Europese cyberbeveiligingscertificaten en het klachtenbeheer in dit verband door de autoriteit bedoeld in artikel 5, § 1;
2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties overeenkomstig de hoofdstukken 5 en 6;	2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties overeenkomstig de hoofdstukken 5 en 6;
3° de deelname aan de EGC van de autoriteit bedoeld in artikel 5, § 1, of van elke andere overheid die hierom verzoekt;	3° de deelname aan de EGC van de autoriteit bedoeld in artikel 5, § 1, of van elke andere overheid die hierom verzoekt;
4° de samenwerking met de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, in artikel 7, §§ 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, of in de artikelen 2, eerste lid, 1° en 9°, en 15, §§ 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-	4° de samenwerking met de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in **de artikelen 3, 2° en 33, van de wet van … betreffende de weerbaarheid van kritieke entiteiten of artikel 15, § 2, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid,** of in de artikelen 2, eerste lid, 1° en 9°, die bevoegd zijn naargelang de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening, in het kader van hun bevoegdheden bedoeld in artikel 24, §

proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening, in het kader van hun bevoegdheden bedoeld in artikel 24, § 1, van de voormelde wet van 1 juli 2011 of in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, van de voormelde wet van 7 april 2019;	1, van de voormelde wet van 1 juli 2011 **of in artikelen 15, § 2, en 24 van de voormelde wet van 26 april 2024;**
5° de samenwerking met de overheden die belast zijn met specifieke opdrachten inzake cyberbeveiliging, als bedoeld in artikel 2, 1), van de Cyberbeveiligingsverordening, overeenkomstig artikel 58, lid 7, onder a), c) en h), van dezelfde verordening.	5° de samenwerking met de overheden die belast zijn met specifieke opdrachten inzake cyberbeveiliging, als bedoeld in artikel 2, 1), van de Cyberbeveiligingsverordening, overeenkomstig artikel 58, lid 7, onder a), c) en h), van dezelfde verordening.
§ 2. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen zijn elk verantwoordelijk voor de verwerkingen die ze uitvoeren voor de verwezenlijking van de doeleinden bedoeld in paragraaf 1.	§ 2. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in de hoofdstukken 5 en 6 door de Koning is aangewezen zijn elk verantwoordelijk voor de verwerkingen die ze uitvoeren voor de verwezenlijking van de doeleinden bedoeld in paragraaf 1.
§ 3. De verwerkingsverantwoordelijken bedoeld in paragraaf 2 verwerken de volgende categorieën van persoonsgegevens:	§ 3. De verwerkingsverantwoordelijken bedoeld in paragraaf 2 verwerken de volgende categorieën van persoonsgegevens:
1° voor het doeleinde bedoeld in paragraaf 1, 1°: de identificatiegegevens van elke natuurlijke persoon die rechtstreeks betrokken is bij een verzoek om afgifte van een Europees cyberbeveiligingscertificaat of bij een klacht in dit verband door de autoriteit bedoeld in artikel 5, § 1, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres;	1° voor het doeleinde bedoeld in paragraaf 1, 1°: de identificatiegegevens van elke natuurlijke persoon die rechtstreeks betrokken is bij een verzoek om afgifte van een Europees cyberbeveiligingscertificaat of bij een klacht in dit verband door de autoriteit bedoeld in artikel 5, § 1, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres;
2° voor het doeleinde bedoeld in paragraaf 1, 2°: elk persoonsgegeven dat noodzakelijk is voor de uitoefening van de toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6;	2° voor het doeleinde bedoeld in paragraaf 1, 2°: elk persoonsgegeven dat noodzakelijk is voor de uitoefening van de toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6;
3° voor het doeleinde bedoeld in paragraaf 1, 3°: de identificatiegegevens van natuurlijke personen die wensen deel te nemen aan de EGC, namelijk hun naam, hun voornaam, hun adres, hun telefoonnummer en hun e-mailadres;	3° voor het doeleinde bedoeld in paragraaf 1, 3°: de identificatiegegevens van natuurlijke personen die wensen deel te nemen aan de EGC, namelijk hun naam, hun voornaam, hun adres, hun telefoonnummer en hun e-mailadres;
4° voor het doeleinde bedoeld in paragraaf 1, 4°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres, of de elektronische-communicatiegegevens als bedoeld in artikel 2,	4° voor het doeleinde bedoeld in paragraaf 1, 4°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres, of de elektronische-communicatiegegevens als bedoeld in artikel 2,

91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken;	91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken;
5° voor het doeleinde bedoeld in paragraaf 1, 5°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres of de elektronische-communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken.	5° voor het doeleinde bedoeld in paragraaf 1, 5°: de identificatiegegevens, namelijk de naam, de voornaam, het adres, het telefoonnummer en het e-mailadres of de elektronische-communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, die rechtstreeks verband houden met de dienstverlener of leverancier van het ICT-product, de ICT-dienst of het ICT-proces in kwestie als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening en verzameld worden door de inspectiedienst in het kader van zijn toezichts- en sanctieopdrachten bedoeld in de hoofdstukken 5 en 6, waarbij deze gegevens geen betrekking mogen hebben op natuurlijke personen die klant zijn van de betrokken houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen, of op de persoonsgegevens die deze klanten verwerken.
In het geval bedoeld in het eerste lid, in de bepaling onder 2°, mogen de persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, en de persoonsgegevens die deze klanten verwerken, slechts worden verwerkt indien ze noodzakelijk zijn voor de toezichtsopdrachten bedoeld in hoofdstuk 5.	In het geval bedoeld in het eerste lid, in de bepaling onder 2°, mogen de persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, en de persoonsgegevens die deze klanten verwerken, slechts worden verwerkt indien ze noodzakelijk zijn voor de toezichtsopdrachten bedoeld in hoofdstuk 5.
Indien mogelijk worden de gegevens bedoeld in het tweede lid gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met Verordening (EU)	Indien mogelijk worden de gegevens bedoeld in het tweede lid gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met Verordening (EU)

2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) of de wetten en reglementen die deze verordening aanvullen of verduidelijken.	2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) of de wetten en reglementen die deze verordening aanvullen of verduidelijken.
§ 4. Onverminderd paragraaf 3, 2°, mag de informatie-uitwisseling tussen overheden bedoeld in deze wet geen betrekking hebben op persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch op persoonsgegevens die deze klanten verwerken.	§ 4. Onverminderd paragraaf 3, 2°, mag de informatie-uitwisseling tussen overheden bedoeld in deze wet geen betrekking hebben op persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, noch op persoonsgegevens die deze klanten verwerken.
§ 5. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:	§ 5. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van verwerkingen:
1° iedere natuurlijke persoon die optreedt voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of voor een overheid;	1° iedere natuurlijke persoon die optreedt voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of voor een overheid;
2° iedere natuurlijke persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten bedoeld in hoofdstuk 5;	2° iedere natuurlijke persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten bedoeld in hoofdstuk 5;
3° iedere natuurlijke persoon die een klacht indient;	3° iedere natuurlijke persoon die een klacht indient;
4° iedere natuurlijke persoon die deelneemt aan de EGC;	4° iedere natuurlijke persoon die deelneemt aan de EGC;
5° iedere natuurlijke persoon wiens persoonsgegevens gebruikt worden in ICT-producten, ICT-diensten of ICT-processen als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening.	5° iedere natuurlijke persoon wiens persoonsgegevens gebruikt worden in ICT-producten, ICT-diensten of ICT-processen als bedoeld in artikel 2, 12) tot 14), van de Cyberbeveiligingsverordening.

Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 14	Art. 14
§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische	§ 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische

communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur , met betrekking tot de sector digitale infrastructuren in de zin van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, met betrekking tot het tegengaan van de verspreiding van terroristische online-inhoud in de zin van de Verordening (EU) 2021/784 van het Europees Parlement en Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, met betrekking tot de tussenhandeldiensten, met betrekking tot artikel XI.216/2, § 2, van het Wetboek van economisch recht en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:	communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur, met betrekking tot de sector digitale infrastructuren in de zin van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, **met betrekking tot de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, in de zin van de wet van … betreffende de weerbaarheid van kritieke entiteiten**, met betrekking tot het tegengaan van de verspreiding van terroristische online-inhoud in de zin van de Verordening (EU) 2021/784 van het Europees Parlement en Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, met betrekking tot de tussenhandeldiensten, met betrekking tot artikel XI.216/2, § 2, van het Wetboek van economisch recht, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:
1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister, van de minister bevoegd voor Economie en van het regeringslid bevoegd voor de Digitale Agenda, binnen het kader van hun respectieve bevoegdheden, of van de Kamer van volksvertegenwoordigers;	1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister, van de minister bevoegd voor Economie en van het regeringslid bevoegd voor de Digitale Agenda, binnen het kader van hun respectieve bevoegdheden, of van de Kamer van volksvertegenwoordigers;
2° het nemen van administratieve beslissingen;	2° het nemen van administratieve beslissingen;
3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:	3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:
a) de wet van 13 juni 2005 betreffende de elektronische communicatie;	a) de wet van 13 juni 2005 betreffende de elektronische communicatie;
b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
c) de wet van 26 januari 2018 betreffende de postdiensten met uitzondering van de artikelen 3, § 2, vijfde lid, 5, § 1, 5/2, 5/3, 5/4, 5/5 en 10/1;	c) de wet van 26 januari 2018 betreffende de postdiensten met uitzondering van de artikelen 3, § 2, vijfde lid, 5, § 1, 5/2, 5/3, 5/4, 5/5 en 10/1;

d) de artikelen 14, § 2, 2°, 15 , 15/1 en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	d) de artikelen 14, § 2, 2°, 15, 15/1 en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;	f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;
g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;	g) **de wet van … betreffende de weerbaarheid van kritieke entiteiten, wat de sector digitale infrastructuren, met uitzondering van de verleners van vertrouwensdiensten, betreft;**
h) de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid en de sectorale inspectiedienst voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet;	h) de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, voor wat betreft de taken toegewezen aan de sectorale overheid en de sectorale inspectiedienst voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet;
i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie;	i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie;
j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie;	j) elke bindende rechtshandeling in het Europese Unierecht, die opdrachten toewijst aan de nationale regelgevende instantie in de sector van de post of elektronische communicatie;
k) elk bindend besluit aangenomen door:	k) elk bindend besluit aangenomen door:
i) het Instituut;	i) het Instituut;

ii) de ministers op basis van artikel 105, § 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie; iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;	ii) de ministers op basis van artikel 105, § 6, eerste lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie; iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;
l) de Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, onverminderd de taken die aan andere bevoegde autoriteiten zijn toevertrouwd krachtens artikel 12, lid 1, a) en b), van die verordening;	l) de Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, onverminderd de taken die aan andere bevoegde autoriteiten zijn toevertrouwd krachtens artikel 12, lid 1, a) en b), van die verordening;
m) de digitaledienstenverordening.	m) de digitaledienstenverordening.
Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.	Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.
4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten,) het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;	4° in geval van een geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, (of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten), het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut;
4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten of in het geval van het uitblijven van akkoord in de zin van artikel XI.216/2, § 2, van het Wetboek van economisch	4° /1 in geval van geschil tussen aanbieders van elektronische-communicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten of in het geval van het uitblijven van akkoord in de zin van artikel XI.216/2, § 2, van het Wetboek van economisch

recht, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;	recht, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.	5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie.
6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1*bis*, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract;	6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1*bis*, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract;
7° het uitoefenen van de toezichts- en sanctieopdrachten uit die hem zijn toevertrouwd bij het koninklijk besluit dat voorziet in de uitvoering van artikel 5, § 2, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.	7° het uitoefenen van de toezichts- en sanctieopdrachten uit die hem zijn toevertrouwd bij het koninklijk besluit dat voorziet in de uitvoering van artikel 5, § 2, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.
Voor de toepassing van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid in de zin van artikel 8, 54°, van dezelfde wet en als sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet, en voor de sector post- en koeriersdiensten.	Voor de toepassing van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid in de zin van artikel 8, 54°, van dezelfde wet en als sectorale inspectiedienst in de zin van artikel 44, § 1, tweede lid, van dezelfde wet voor de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten in de zin van artikel 8, 24°, van dezelfde wet, en voor de sector post- en koeriersdiensten.

§ 1/1. Wat de federale bevoegdheden betreft, is het Instituut een bevoegde autoriteit in de zin van artikel 49 van de digitaledienstenverordening.	§ 1/1. Wat de federale bevoegdheden betreft, is het Instituut een bevoegde autoriteit in de zin van artikel 49 van de digitaledienstenverordening.
§ 2. In het kader van zijn bevoegdheden:	§ 2. In het kader van zijn bevoegdheden:
1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;	1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten (met inbegrip van met name consumenten met een handicap), fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie;
2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;	2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld;
3° werkt het Instituut samen met en verstrekt het informatie aan:	3° werkt het Instituut samen met en verstrekt het informatie aan:
a) de Europese Commissie, ENISA, het Bureau, Berec en aan de Europese Raad voor digitale diensten;	a) de Europese Commissie, ENISA, het Bureau, Berec en aan de Europese Raad voor digitale diensten;
b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;	b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie;
c) de regulerende instanties in de overige economische sectoren;	c) de regulerende instanties in de overige economische sectoren;
d) de federale overheidsdiensten die belast zijn met consumentenbescherming;	d) de federale overheidsdiensten die belast zijn met consumentenbescherming;

e) de Belgische instanties die belast zijn met mededinging.	e) de Belgische instanties die belast zijn met mededinging.
De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;	De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut;
f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;	f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus;
g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, met inbegrip van de beveiliging van netwerk- en informatiesystemen, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;	g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, met inbegrip van de beveiliging van netwerk- en informatiesystemen,of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land;
h) de Gegevensbeschermingsautoriteit;	h) de Gegevensbeschermingsautoriteit;
i) de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;	i) de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;
De Koning kan, na raadpleging van het Instituut en op gezamenlijk voorstel van de minister bevoegd voor Economie en van de minister, de nadere regels vastleggen van de samenwerking, raadpleging en uitwisseling van informatie tussen de in het eerste lid bedoelde Federale Overheidsdienst en het Instituut;	De Koning kan, na raadpleging van het Instituut en op gezamenlijk voorstel van de minister bevoegd voor Economie en van de minister, de nadere regels vastleggen van de samenwerking, raadpleging en uitwisseling van informatie tussen de in het eerste lid bedoelde Federale Overheidsdienst en het Instituut;
j) de ministers bedoeld in artikel 105, § 1, derde lid, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel;	j) de ministers bedoeld in artikel 105, § 1, derde lid, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel;
k) het federaal parket en de bevoegde autoriteiten van de andere lidstaten bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud;	k) het federaal parket en de bevoegde autoriteiten van de andere lidstaten bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud;

l) de sociaal inspecteurs van de Algemene Directie Toezicht op de Sociale Wetten van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg, de sociaal inspecteurs van de Rijksdienst voor Sociale Zekerheid, de sociaal inspecteurs van de Rijksdienst voor Arbeidsvoorziening en de sociaal inspecteurs van het Rijksinstituut voor de sociale verzekeringen der zelfstandigen;	l) de sociaal inspecteurs van de Algemene Directie Toezicht op de Sociale Wetten van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg, de sociaal inspecteurs van de Rijksdienst voor Sociale Zekerheid, de sociaal inspecteurs van de Rijksdienst voor Arbeidsvoorziening en de sociaal inspecteurs van het Rijksinstituut voor de sociale verzekeringen der zelfstandigen;
m) de digitaledienstencoördinatoren en de andere bevoegde autoriteiten in de zin van artikel 49 van de digitaledienstenverordening;	m) de digitaledienstencoördinatoren en de andere bevoegde autoriteiten in de zin van artikel 49 van de digitaledienstenverordening;
4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;	4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993;
5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.	5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden.
6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald:	6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in artikel 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 35 van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald:
- waken over de kwaliteit en het voortbestaan van de universele dienst;	- waken over de kwaliteit en het voortbestaan van de universele dienst;

- waken over de belangen van de gebruikers van postdiensten; - bijdragen tot de ontwikkeling van een interne markt voor postdiensten; - het bevorderen van de concurrentie in de postsector;	- waken over de belangen van de gebruikers van postdiensten; - bijdragen tot de ontwikkeling van een interne markt voor postdiensten; - het bevorderen van de concurrentie in de postsector;
7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de exploitant eisen op elk moment, in afwijking van artikel 25, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.	**Opgeheven.**
§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.	§ 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten.
§ 4. Op voorstel van het Instituut of op gezamenlijk voorstel van de minister bevoegd voor Economie, van het regeringslid bevoegd voor de Digitale Agenda en van de minister, na advies van het Instituut, kan de Koning de nadere regels vaststellen van de samenwerking, raadpleging en uitwisseling van informatie tussen het Instituut en de andere sectorale overheden die nog niet onder paragraaf 2, 3°, vallen, wanneer dit nuttig is voor een doeltreffende toepassing van de digitaledienstenverordening.	§ 4. Op voorstel van het Instituut of op gezamenlijk voorstel van de minister bevoegd voor Economie, van het regeringslid bevoegd voor de Digitale Agenda en van de minister, na advies van het Instituut, kan de Koning de nadere regels vaststellen van de samenwerking, raadpleging en uitwisseling van informatie tussen het Instituut en de andere sectorale overheden die nog niet onder paragraaf 2, 3°, vallen, wanneer dit nuttig is voor een doeltreffende toepassing van de digitaledienstenverordening.

Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 36/14	Art. 36/14
§ 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen die zij ontvangen heeft in het kader van de uitvoering van haar in artikel 36/2, § 1 bedoelde opdrachten:	§ 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen die zij ontvangen heeft in het kader van de uitvoering van haar in artikel 36/2, § 1 bedoelde opdrachten:
1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een	1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een

soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.	soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen.
Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen, kan de Bank gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samen-hangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.	Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen, kan de Bank gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samen-hangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.
In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen;	In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen;
2° binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de	2° binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de

artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij de GTM-verordening;	artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij de GTM-verordening;
2° /1 binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van andere lidstaten van de Europese Economische Ruimte die één of meerdere toezichtsbevoegdheden uitoefenen ten aanzien van de onderworpen entiteiten die worden opgesomd in artikel 2, lid 1, punten 1) en 2) van richtlijn (EU) 2015/849, met het oog op de naleving van die richtlijn en in het kader van de uitvoering van de opdracht die hen is opgedragen bij die richtlijn;	2° /1 binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten van andere lidstaten van de Europese Economische Ruimte die één of meerdere toezichtsbevoegdheden uitoefenen ten aanzien van de onderworpen entiteiten die worden opgesomd in artikel 2, lid 1, punten 1) en 2) van richtlijn (EU) 2015/849, met het oog op de naleving van die richtlijn en in het kader van de uitvoering van de opdracht die hen is opgedragen bij die richtlijn;
3° met inachtneming van het recht van de Europese Unie, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3 , met inbegrip van de autoriteiten die soortgelijke bevoegdheden hebben als de in de bepaling onder 2° /1 bedoelde autoriteiten, en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;	3° met inachtneming van het recht van de Europese Unie, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de autoriteiten die soortgelijke bevoegdheden hebben als de in de bepaling onder 2° /1 bedoelde autoriteiten, en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;
4° aan de FSMA;	4° aan de FSMA;
5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling;	5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling;
6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereglementeerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te	6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereglementeerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te

vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;	vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;
7° binnen de grenzen van het recht van de Europese Unie, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten;	7° binnen de grenzen van het recht van de Europese Unie, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten;
8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld;	8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld;
9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen;	9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen;
10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd;	10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd;
11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan;	11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan;
12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit;	12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit;
13° …	13° …
14° aan de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën, indien het recht van de Europese Unie of een wettelijke of reglementaire bepaling inzake financiële sancties (met name de bindende bepalingen betreffende financiële	14° aan de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën, indien het recht van de Europese Unie of een wettelijke of reglementaire bepaling inzake financiële sancties (met name de bindende bepalingen betreffende financiële

embargo's die in artikel 4, 6°, van de wet van 18 september 2017 zijn opgenomen) in de mededeling van vertrouwelijke informatie voorziet, of wanneer de Algemene Administratie van de Thesaurie optreedt als autoriteit die toezicht houdt op de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;	embargo's die in artikel 4, 6°, van de wet van 18 september 2017 zijn opgenomen) in de mededeling van vertrouwelijke informatie voorziet, of wanneer de Algemene Administratie van de Thesaurie optreedt als autoriteit die toezicht houdt op de naleving van Verordening (EG) nr. 2271/96 van de Raad van 22 november 1996 tot bescherming tegen de gevolgen van de extraterritoriale toepassing van rechtsregels uitgevaardigd door een derde land en daarop gebaseerde of daaruit voortvloeiende handelingen;
15° binnen de grenzen van het recht van de Europese Unie, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;	15° binnen de grenzen van het recht van de Europese Unie, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;
16° aan Fedris;	16° aan Fedris;
17° binnen de grenzen van het recht van de Europese Unie, aan de Federale Overheidsdienst Economie, in zijn hoedanigheid van bevoegde autoriteit voor het toezicht op de naleving van de bepalingen van boek VII, titels 1 tot 3, titel 5, hoofdstuk 1, en titels 6 en 7 van het Wetboek van economisch recht, en aan de ambtenaren aangesteld door de minister die in het raam van hun opdracht bedoeld in artikel XV.2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV.89 van het voornoemde Wetboek op te sporen en vast te stellen;	17° binnen de grenzen van het recht van de Europese Unie, aan de Federale Overheidsdienst Economie, in zijn hoedanigheid van bevoegde autoriteit voor het toezicht op de naleving van de bepalingen van boek VII, titels 1 tot 3, titel 5, hoofdstuk 1, en titels 6 en 7 van het Wetboek van economisch recht, en aan de ambtenaren aangesteld door de minister die in het raam van hun opdracht bedoeld in artikel XV.2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV.89 van het voornoemde Wetboek op te sporen en vast te stellen;
18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010;	18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010;
19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en	19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en

bedrijfspensioenen en aan de Europese Bankautoriteit;	bedrijfspensioenen en aan de Europese Bankautoriteit;
20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren zulks vereist;	20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van **artikel 26 van de wet van … betreffende de weerbaarheid van kritieke entiteiten zulks vereist;**
20° /1 binnen de grenzen van het recht van de Europese Unie, aan de politiediensten en aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 46°, van dezelfde wet ten behoeve van de tenuitvoerlegging van artikel 53, § 2, van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;	20° /1 binnen de grenzen van het recht van de Europese Unie, aan de politiediensten en aan de nationale cyberbeveiligingsautoriteit bedoeld in artikel 8, 45°, van de NIS2-wet en aan het nationaal CSIRT bedoeld in artikel 8, 46°, van dezelfde wet ten behoeve van de tenuitvoerlegging van artikel 53, § 2, van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;
20°/2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, of aan de door de Koning krachtens artikel 5, § 2, van dezelfde wet aangewezen overheden;	20°/2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, of aan de door de Koning krachtens artikel 5, § 2, van dezelfde wet aangewezen overheden;
21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van	21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van

onderlinge bijstand als bedoeld in artikel 43*bis*, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen;	onderlinge bijstand als bedoeld in artikel 43*bis*, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen;
22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12*ter*, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel;	22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12*ter*, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel;
22° /1 binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten bedoeld in artikel 3 van Verordening 2021/23, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die bedoeld in artikel 12*ter*, § 1/1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk blijkt voor het plannen of uitvoeren van een afwikkelingsmaatregel;	22° /1 binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten bedoeld in artikel 3 van Verordening 2021/23, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die bedoeld in artikel 12*ter*, § 1/1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk blijkt voor het plannen of uitvoeren van een afwikkelingsmaatregel;
23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtsopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name:	23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtsopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name:
a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen;	a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen;
b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het	b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het

statuut van en het toezicht op kredietinstellingen; en	statuut van en het toezicht op kredietinstellingen; en
c) de speciaal commissaris en de voorlopige bestuurder als bedoeld in artikel 236, § 1 van de voornoemde wet van 25 april 2014, artikel 204, § 1 van de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, artikel 517, § 1 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, de artikelen 117, § 1 en 215, § 1 van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, artikel 48, eerste lid van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling, en de artikelen 36/30, § 1, tweede lid en 36/30/1, § 2 van deze wet;	c) de speciaal commissaris en de voorlopige bestuurder als bedoeld in artikel 236, § 1 van de voornoemde wet van 25 april 2014, artikel 204, § 1 van de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen, artikel 517, § 1 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, de artikelen 117, § 1 en 215, § 1 van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, artikel 48, eerste lid van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling, en de artikelen 36/30, § 1, tweede lid en 36/30/1, § 2 van deze wet;
24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 15 van de NIS2-wet voor de uitvoering van de bepalingen van de NIS2-wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;
25° aan de Federale Overheidsdienst Economie, KMO, Middenstand en Energie, in het kader van de uitvoering van zijn opdracht bedoeld in artikel 85, § 1, 5°, van de wet van 18 september 2017 ten aanzien van de entiteiten bedoeld in artikel 5, § 1, 21°, van dezelfde wet;	25° aan de Federale Overheidsdienst Economie, KMO, Middenstand en Energie, in het kader van de uitvoering van zijn opdracht bedoeld in artikel 85, § 1, 5°, van de wet van 18 september 2017 ten aanzien van de entiteiten bedoeld in artikel 5, § 1, 21°, van dezelfde wet;
26° binnen de grenzen van het recht van de Europese Unie, aan de financiële inlichtingeneenheden bedoeld in artikel 4, 15° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;	26° binnen de grenzen van het recht van de Europese Unie, aan de financiële inlichtingeneenheden bedoeld in artikel 4, 15° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
27° ingeval de financiële situatie van een financiële instelling als bedoeld in artikel 36/2 verslechtert, aan het openbaar ministerie;	27° ingeval de financiële situatie van een financiële instelling als bedoeld in artikel 36/2 verslechtert, aan het openbaar ministerie;

28° binnen de grenzen van het recht van de Europese Unie, aan de Europese Commissie als deze gegevens nodig zijn voor de uitoefening van de bevoegdheden van deze laatste.	28° binnen de grenzen van het recht van de Europese Unie, aan de Europese Commissie als deze gegevens nodig zijn voor de uitoefening van de bevoegdheden van deze laatste.
§ 2. De Bank mag enkel vertrouwelijke informatie krachtens paragraaf 1 meedelen op de volgende voorwaarden:	§ 2. De Bank mag enkel vertrouwelijke informatie krachtens paragraaf 1 meedelen op de volgende voorwaarden:
1° de autoriteiten of instellingen die de informatie ontvangen, gebruiken deze voor de uitvoering van hun opdrachten, met inbegrip van de mededeling van deze informatie aan derden ingevolge een wettelijke verplichting van deze autoriteiten of instellingen; in de andere gevallen kan de Bank toestaan, binnen de grenzen van het recht van de Europese Unie, dat de ontvangers van de informatie deze bekendmaken aan derden, mits de Bank daar voorafgaandelijk mee heeft ingestemd en, in voorkomend geval, mits de informatie alleen voor de door de Bank toegestane doeleinden bekendgemaakt wordt;	1° de autoriteiten of instellingen die de informatie ontvangen, gebruiken deze voor de uitvoering van hun opdrachten, met inbegrip van de mededeling van deze informatie aan derden ingevolge een wettelijke verplichting van deze autoriteiten of instellingen; in de andere gevallen kan de Bank toestaan, binnen de grenzen van het recht van de Europese Unie, dat de ontvangers van de informatie deze bekendmaken aan derden, mits de Bank daar voorafgaandelijk mee heeft ingestemd en, in voorkomend geval, mits de informatie alleen voor de door de Bank toegestane doeleinden bekendgemaakt wordt;
2° Wat de aldus aan hen meegedeelde informatie betreft, zijn deze buitenlandse autoriteiten of instellingen aan een beroepsgeheim gebonden dat gelijkwaardig is aan dat van artikel 35; en	2° Wat de aldus aan hen meegedeelde informatie betreft, zijn deze buitenlandse autoriteiten of instellingen aan een beroepsgeheim gebonden dat gelijkwaardig is aan dat van artikel 35; en
3° indien de betrokken informatie afkomstig is van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, mag zij enkel bekendgemaakt worden aan de volgende autoriteiten of instellingen mits de autoriteit die de informatie heeft verstrekt uitdrukkelijk akkoord gaat met deze bekendmaking, en, in voorkomend geval, mits de informatie alleen voor de door deze autoriteit toegestane doeleinden bekendgemaakt wordt:	3° indien de betrokken informatie afkomstig is van een autoriteit van een andere lidstaat van de Europese Economische Ruimte, mag zij enkel bekendgemaakt worden aan de volgende autoriteiten of instellingen mits de autoriteit die de informatie heeft verstrekt uitdrukkelijk akkoord gaat met deze bekendmaking, en, in voorkomend geval, mits de informatie alleen voor de door deze autoriteit toegestane doeleinden bekendgemaakt wordt:
a) de in paragraaf 1, 5°, 6°, 8° en 11°, bedoelde autoriteiten of instellingen;	a) de in paragraaf 1, 5°, 6°, 8° en 11°, bedoelde autoriteiten of instellingen;
b) de in paragraaf 1, 3°, 5°, 8°, 9°, 11°, 18° en 22°, bedoelde autoriteiten of instellingen van derde Staten;	b) de in paragraaf 1, 3°, 5°, 8°, 9°, 11°, 18° en 22°, bedoelde autoriteiten of instellingen van derde Staten;
c) autoriteiten of instellingen van derde Staten die opdrachten uitvoeren die gelijkwaardig zijn aan die van de FSMA.	c) autoriteiten of instellingen van derde Staten die opdrachten uitvoeren die gelijkwaardig zijn aan die van de FSMA.

§ 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in paragraaf 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van paragraaf 1, gebonden door het beroepsgeheim als bedoeld in artikel 35.	§ 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in paragraaf 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van paragraaf 1, gebonden door het beroepsgeheim als bedoeld in artikel 35.
Art. 36/49	Art. 36/49
De Bank wordt aangeduid als administratieve overheid in de zin van artikel 22quinquies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. De Bank is bevoegd voor de entiteiten van de sector financiën die zij als kritieke infrastructuur identificeert krachtens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.	De Bank wordt aangeduid als administratieve overheid in de zin van artikel 22quinquies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. De Bank is bevoegd voor de entiteiten van de sector financiën die zij als **kritieke entiteit** identificeert krachtens **de wet van … betreffende de weerbaarheid van kritieke entiteiten.**

Wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen

Art. 15/2*sexies*	Art. 15/2*sexies*
§ 1. Elke beheerder van niet-actieve infrastructuur heeft het recht ondernemingen die elektronische communicatienetwerken aanbieden of waaraan een vergunning voor het aanbieden ervan is verleend, toegang te geven tot zijn niet-actieve infrastructuur met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid.	§ 1. Elke beheerder van niet-actieve infrastructuur heeft het recht ondernemingen die elektronische communicatienetwerken aanbieden of waaraan een vergunning voor het aanbieden ervan is verleend, toegang te geven tot zijn niet-actieve infrastructuur met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid.
§ 2. Op schriftelijk verzoek van een onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, willigt de beheerder van niet-actieve infrastructuur de redelijke verzoeken om toegang tot zijn niet-actieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een tijdschema.	§ 2. Op schriftelijk verzoek van een onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, willigt de beheerder van niet-actieve infrastructuur de redelijke verzoeken om toegang tot zijn niet-actieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een tijdschema.

§ 3. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:	§ 3. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:
1° de technische geschiktheid van de niet-actieve infrastructuur waarvoor om toegang wordt verzocht voor het onderbrengen van de in paragraaf 2 bedoelde elementen van elektronische communicatienetwerken met hoge snelheid;	1° de technische geschiktheid van de niet-actieve infrastructuur waarvoor om toegang wordt verzocht voor het onderbrengen van de in paragraaf 2 bedoelde elementen van elektronische communicatienetwerken met hoge snelheid;
2° de beschikbaarheid van ruimte om andere elementen van het vervoernet, van het gesloten industrieel net of van de directe leiding van de beheerder van niet-actieve infrastructuur te huisvesten, de toekomstige behoeften aan ruimte van de beheerder inbegrepen, of om de in paragraaf 2 bedoelde elementen van de elektronische communicatienetwerken met hoge snelheid te huisvesten, waarbij onder meer rekening wordt gehouden met de toekomstige behoeften aan ruimte, die afdoende moeten worden aangetoond, van de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, die het verzoek heeft ingediend of met de elementen van netwerken van andere ondernemingen;	2° de beschikbaarheid van ruimte om andere elementen van het vervoernet, van het gesloten industrieel net of van de directe leiding van de beheerder van niet-actieve infrastructuur te huisvesten, de toekomstige behoeften aan ruimte van de beheerder inbegrepen, of om de in paragraaf 2 bedoelde elementen van de elektronische communicatienetwerken met hoge snelheid te huisvesten, waarbij onder meer rekening wordt gehouden met de toekomstige behoeften aan ruimte, die afdoende moeten worden aangetoond, van de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, die het verzoek heeft ingediend of met de elementen van netwerken van andere ondernemingen;
3° overwegingen met betrekking tot veiligheid en volksgezondheid;	3° overwegingen met betrekking tot veiligheid en volksgezondheid;
4° de integriteit en veiligheid van de niet-actieve infrastructuur, met name van kritieke nationale infrastructuur bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	4° de integriteit en veiligheid van de niet-actieve infrastructuur, met name van **kritieke entiteiten** bedoeld in **de wet van … betreffende de weerbaarheid van kritieke entiteiten**;
5° het risico van ernstige verstoring van de geplande elektronische communicatiediensten wanneer andere diensten via de niet-actieve infrastructuur worden verstrekt;	5° het risico van ernstige verstoring van de geplande elektronische communicatiediensten wanneer andere diensten via de niet-actieve infrastructuur worden verstrekt;
6° de vraag of de beheerder van de niet-actieve infrastructuur beschikt over levensvatbare alternatieve middelen voor het verlenen van wholesaletoegang tot de fysieke niet-actieve infrastructuur die geschikt zijn voor het aanbieden van elektronische communicatienetwerken met hoge snelheid, op	6° de vraag of de beheerder van de niet-actieve infrastructuur beschikt over levensvatbare alternatieve middelen voor het verlenen van wholesaletoegang tot de fysieke niet-actieve infrastructuur die geschikt zijn voor het aanbieden van elektronische communicatienetwerken met hoge snelheid, op

voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.	voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.
Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de beheerder van de niet-actieve infrastructuur de redenen voor de weigering op.	Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de beheerder van de niet-actieve infrastructuur de redenen voor de weigering op.
§ 4. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar de instantie voor geschillenbeslechting inzake netwerkinfrastructuur.	§ 4. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar de instantie voor geschillenbeslechting inzake netwerkinfrastructuur.
Het eerste lid is van toepassing onverminderd de mogelijkheid voor elke partij om bij geschillen de zaak aanhangig te maken bij de rechtbank van eerste aanleg te Brussel, die beslist als in kort geding, overeenkomstig de procedure die bepaald is in artikel 15/2*decies*.	Het eerste lid is van toepassing onverminderd de mogelijkheid voor elke partij om bij geschillen de zaak aanhangig te maken bij de rechtbank van eerste aanleg te Brussel, die beslist als in kort geding, overeenkomstig de procedure die bepaald is in artikel 15/2*decies*.
§ 5. Dit artikel laat het eigendomsrecht van de eigenaar van de niet-actieve infrastructuur, indien de beheerder van de niet-actieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, om de toelatingen en vergunningen te bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn elektronisch communicatienetwerk met hoge snelheid, onverlet.	§ 5. Dit artikel laat het eigendomsrecht van de eigenaar van de niet-actieve infrastructuur, indien de beheerder van de niet-actieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, om de toelatingen en vergunningen te bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn elektronisch communicatienetwerk met hoge snelheid, onverlet.
Wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt	
Art. 14/1	Art. 14/1
§ 1. Elke beheerder van niet-actieve infrastructuur heeft het recht ondernemingen die elektronische communicatienetwerken aanbieden of waaraan een vergunning voor het aanbieden ervan is verleend, toegang te geven tot zijn niet-actieve infrastructuur met het oog	§ 1. Elke beheerder van niet-actieve infrastructuur heeft het recht ondernemingen die elektronische communicatienetwerken aanbieden of waaraan een vergunning voor het aanbieden ervan is verleend, toegang te geven tot zijn niet-actieve infrastructuur met het oog

op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid.	op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid.
§ 2. Op schriftelijk verzoek van een onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, willigt de beheerder van niet-actieve infrastructuur voldoen aan redelijke verzoeken om toegang tot zijn niet-actieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een tijdschema.	§ 2. Op schriftelijk verzoek van een onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, willigt de beheerder van niet-actieve infrastructuur voldoen aan redelijke verzoeken om toegang tot zijn niet-actieve infrastructuur in onder billijke en redelijke eisen en voorwaarden met inbegrip van de prijs, met het oog op de aanleg van elementen van elektronische communicatienetwerken met hoge snelheid. Dat schriftelijke verzoek bevat een nadere omschrijving van de elementen van het project waarvoor om toegang wordt verzocht, met inbegrip van een tijdschema.
§ 3. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:	§ 3. Elke weigering om toegang te verlenen, is gebaseerd op objectieve, transparante en evenredige criteria, zoals:
1° de technische geschiktheid van de niet-actieve infrastructuur voor het onderbrengen van de in paragraaf 2 bedoelde elementen van elektronische communicatienetwerken met hoge snelheid;	1° de technische geschiktheid van de niet-actieve infrastructuur voor het onderbrengen van de in paragraaf 2 bedoelde elementen van elektronische communicatienetwerken met hoge snelheid;
2° de beschikbaarheid van ruimte om andere elementen van het transmissienet, van het gesloten industrieel net, van de aansluiting of van de directe leiding van de beheerder van niet-actieve infrastructuur te huisvesten, de toekomstige behoeften aan ruimte van de beheerder inbegrepen, of om de in paragraaf 2 bedoelde elementen van de elektronische communicatienetwerken met hoge snelheid te huisvesten, waarbij onder meer rekening wordt gehouden met de toekomstige behoeften aan ruimte, die afdoende moeten worden aangetoond, van de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend en die het verzoek heeft ingediend of met de elementen van netwerken van andere ondernemingen;	2° de beschikbaarheid van ruimte om andere elementen van het transmissienet, van het gesloten industrieel net, van de aansluiting of van de directe leiding van de beheerder van niet-actieve infrastructuur te huisvesten, de toekomstige behoeften aan ruimte van de beheerder inbegrepen, of om de in paragraaf 2 bedoelde elementen van de elektronische communicatienetwerken met hoge snelheid te huisvesten, waarbij onder meer rekening wordt gehouden met de toekomstige behoeften aan ruimte, die afdoende moeten worden aangetoond, van de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend en die het verzoek heeft ingediend of met de elementen van netwerken van andere ondernemingen;
3° overwegingen met betrekking tot veiligheid en volksgezondheid;	3° overwegingen met betrekking tot veiligheid en volksgezondheid;
4° de integriteit en veiligheid van de niet-actieve infrastructuur, met name van kritieke nationale	4° de integriteit en veiligheid van de niet-actieve infrastructuur, met name van **kritieke entiteiten**

infrastructuur bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	bedoeld in **de wet van … betreffende de weerbaarheid van kritieke entiteiten;**
5° het risico van ernstige verstoring van de geplande elektronische communicatiediensten wanneer andere diensten via de niet-actieve infrastructuur worden verstrekt;	5° het risico van ernstige verstoring van de geplande elektronische communicatiediensten wanneer andere diensten via de niet-actieve infrastructuur worden verstrekt;
6° de vraag of de beheerder van de niet-actieve infrastructuur beschikt over levensvatbare alternatieve middelen voor het verlenen van wholesaletoegang tot de fysieke niet-actieve infrastructuur die geschikt zijn voor het aanbieden van elektronische communicatienetwerken met hoge snelheid, op voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.	6° de vraag of de beheerder van de niet-actieve infrastructuur beschikt over levensvatbare alternatieve middelen voor het verlenen van wholesaletoegang tot de fysieke niet-actieve infrastructuur die geschikt zijn voor het aanbieden van elektronische communicatienetwerken met hoge snelheid, op voorwaarde dat de toegang onder billijke en redelijke voorwaarden wordt verleend.
Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de beheerder van de niet-actieve infrastructuur de redenen voor de weigering op.	Uiterlijk twee maanden vanaf de datum van ontvangst van het volledige verzoek om toegang geeft de beheerder van de niet-actieve infrastructuur de redenen voor de weigering op.
§ 4. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar de instantie voor geschillenbeslechting inzake netwerkinfrastructuur.	§ 4. Indien uiterlijk twee maanden vanaf de datum van ontvangst van het verzoek, toegang wordt geweigerd of geen overeenstemming wordt bereikt over specifieke eisen en voorwaarden, met inbegrip van de prijs, heeft elke partij het recht deze kwestie door te verwijzen naar de instantie voor geschillenbeslechting inzake netwerkinfrastructuur.
Het eerste lid is van toepassing onverminderd de mogelijkheid voor elke partij om bij geschillen de zaak aanhangig te maken bij de rechtbank van eerste aanleg te Brussel, die beslist als in kort geding, overeenkomstig de procedure die bepaald is in artikel 14/5.	Het eerste lid is van toepassing onverminderd de mogelijkheid voor elke partij om bij geschillen de zaak aanhangig te maken bij de rechtbank van eerste aanleg te Brussel, die beslist als in kort geding, overeenkomstig de procedure die bepaald is in artikel 14/5.
§ 5. Dit artikel laat het eigendomsrecht van de eigenaar van de niet-actieve infrastructuur, indien de beheerder van de niet-actieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, om de toelatingen en vergunningen te	§ 5. Dit artikel laat het eigendomsrecht van de eigenaar van de niet-actieve infrastructuur, indien de beheerder van de niet-actieve infrastructuur niet de eigenaar is, alsmede het eigendomsrecht van derden, zoals landeigenaren en eigenaren van privaat eigendom, onverlet. Dit artikel laat eveneens de verplichting voor de onderneming die openbare communicatienetwerken aanbiedt of waaraan een vergunning voor het aanbieden ervan is verleend, om de toelatingen en vergunningen te

bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn elektronisch communicatienetwerk met hoge snelheid, onverlet.	bekomen die vereist zijn voor de aanleg van de bestanddelen van zijn elektronisch communicatienetwerk met hoge snelheid, onverlet.
Strafwetboek	
Art. 546/2	Art. 546/2
§ 1. Het misdrijf bedoeld in art. 546/1 wordt gestraft met gevangenisstraf van acht dagen tot één jaar en met een geldboete van zesentwintig tot duizend euro of met een van die straffen alleen:	§ 1. Het misdrijf bedoeld in art. 546/1 wordt gestraft met gevangenisstraf van acht dagen tot één jaar en met een geldboete van zesentwintig tot duizend euro of met een van die straffen alleen:
1° ingeval van de betrokken activiteit een gewoonte wordt gemaakt;	1° ingeval van de betrokken activiteit een gewoonte wordt gemaakt;
2° indien het gepleegd wordt bij nacht;	2° indien het gepleegd wordt bij nacht;
3° indien het gepleegd wordt door twee of meer personen;	3° indien het gepleegd wordt door twee of meer personen;
4° indien het gepleegd wordt met bedrieglijk opzet of het oogmerk om te schaden.	4° indien het gepleegd wordt met bedrieglijk opzet of het oogmerk om te schaden.
5° indien het gepleegd wordt door middel van geweld of bedreiging;	5° indien het gepleegd wordt door middel van geweld of bedreiging;
6° indien kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren werd binnengegaan of binnengedrongen.	6° **indien een kritieke entiteit, in de zin van de wet van … betreffende de weerbaarheid van kritieke entiteiten werd binnengegaan of binnengedrongen.**
§ 2. Poging tot het plegen van het in § 1 van dit artikel bedoelde misdrijf wordt gestraft met gevangenisstraf van acht dagen tot zes maanden en met een geldboete van zesentwintig euro tot vijfhonderd euro of met een van die straffen alleen.	§ 2. Poging tot het plegen van het in § 1 van dit artikel bedoelde misdrijf wordt gestraft met gevangenisstraf van acht dagen tot zes maanden en met een geldboete van zesentwintig euro tot vijfhonderd euro of met een van die straffen alleen.
Art. 550*ter*	Art. 550*ter*
§ 1. Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig	§ 1. Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig

euro tot vijfentwintigduizend euro of met één van die straffen alleen.	euro tot vijfentwintigduizend euro of met één van die straffen alleen.
Wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt met bedrieglijk opzet of met het oogmerk om te schaden, bedraagt de gevangenisstraf zes maanden tot vijf jaar.	Wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt met bedrieglijk opzet of met het oogmerk om te schaden, bedraagt de gevangenisstraf zes maanden tot vijf jaar.
Dezelfde straf wordt toegepast wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt tegen een informatiesysteem van een kritieke infrastructuur, zoals bedoeld in artikel 3, 4°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.	**Dezelfde straf wordt toegepast wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt tegen een informatiesysteem van een kritieke entiteit zoals bedoeld in artikel 3, 3°, van de wet van … betreffende de weerbaarheid van kritieke entiteiten.**
§ 2. Hij die, ten gevolge van het plegen van een misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig [euro] tot vijfenzeventigduizend [euro] of met een van die straffen alleen.	§ 2. Hij die, ten gevolge van het plegen van een misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig [euro] tot vijfenzeventigduizend [euro] of met een van die straffen alleen.
§ 3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig f rank tot honderdduizend [euro] of met een van die straffen alleen.	§ 3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend [euro] of met een van die straffen alleen.
§ 4. Hij die onrechtmatig enig instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om de in §§ 1 tot 3 bedoelde misdrijven mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig euro tot honderdduizend euro of met één van die straffen alleen.	§ 4. Hij die onrechtmatig enig instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om de in §§ 1 tot 3 bedoelde misdrijven mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig euro tot honderdduizend euro of met één van die straffen alleen.

§ 5. De straffen bepaald in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210bis, 259bis, 314bis, 504quater of 550bis.	§ 5. De straffen bepaald in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210bis, 259bis, 314bis, 504quater of 550bis.
§ 6. Poging tot het plegen van het in § 1 bedoelde misdrijf wordt gestraft met dezelfde straffen.	§ 6. Poging tot het plegen van het in § 1 bedoelde misdrijf wordt gestraft met dezelfde straffen.

Wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 15*bis*	Art. 15*bis*
Overeenkomstig artikel 24 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan, is het Agentschap belast met het controleren van de toepassing van de bepalingen van deze wet op een nucleaire installatie bestemd voor de industriële productie van elektriciteit, voor wat betreft de elementen die dienen voor de transmissie van de elektriciteit en die werden aangeduid als kritieke infrastructuur krachtens bovengenoemde wet van 1 juli 2011. De nadere regels van de controle worden door de Koning geregeld.	Overeenkomstig **artikel 33 van de wet van … betreffende de weerbaarheid van kritieke entiteiten** en de uitvoeringsbesluiten ervan, is het Agentschap belast met het controleren van de toepassing van de bepalingen van deze wet op een nucleaire installatie bestemd voor de industriële productie van elektriciteit, voor wat betreft de elementen die dienen voor de transmissie van de elektriciteit en die werden aangeduid als **kritieke entiteit krachtens de wet van … betreffende de weerbaarheid van kritieke entiteiten.** De nadere regels van de controle worden door de Koning geregeld.

Wet van 10 juli 2006 betreffende de analyse van de dreiging

Art. 6	Art. 6
§ 1. Onverminderd de verplichtingen opgenomen in de internationale rechtsnormen die hen binden, zijn de ondersteunende diensten verplicht, ambtshalve of op vraag van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de inlichtingen betreffende de dreigingen bedoeld in artikel 3, de personen en groeperingen, de daders of mogelijke doelwitten van een dreiging, en de gebeurtenissen, waarover zij in het kader van hun wettelijke opdrachten ter voorkoming en	§ 1. Onverminderd de verplichtingen opgenomen in de internationale rechtsnormen die hen binden, zijn de ondersteunende diensten verplicht, ambtshalve of op vraag van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en de inlichtingen betreffende de dreigingen bedoeld in artikel 3, de personen en groeperingen, de daders of mogelijke doelwitten van een dreiging, en de gebeurtenissen, waarover zij in het kader van hun wettelijke opdrachten ter voorkoming en

ter opvolging van het terrorisme en het extremisme beschikken in de zin van artikel 8, 1°, b) en c), van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten en die relevant zijn om de doeleinden te verwezenlijken van de gemeenschappelijke evaluaties bedoeld in artikel 8, eerste lid, 1° en 2°, mee te delen.	ter opvolging van het terrorisme en het extremisme beschikken in de zin van artikel 8, 1°, b) en c), van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten en die relevant zijn om de doeleinden te verwezenlijken van de gemeenschappelijke evaluaties bedoeld in artikel 8, eerste lid, 1° en 2°, mee te delen.
Wanneer er gronden zijn om aan te nemen dat de integriteit van natuurlijke personen in concreet en onmiddellijk gevaar is, in verband met extremistische en terroristische dreigingen, kan de directeur van de ondersteunende diensten eisen om de persoonsgegevens en de inlichtingen bedoeld in het eerste lid onmiddellijk mee te delen. De directeur motiveert zijn verzoek inzake de noodzaak om de persoonsgegevens en de inlichtingen onmiddellijk toe te sturen.	Wanneer er gronden zijn om aan te nemen dat de integriteit van natuurlijke personen in concreet en onmiddellijk gevaar is, in verband met extremistische en terroristische dreigingen, kan de directeur van de ondersteunende diensten eisen om de persoonsgegevens en de inlichtingen bedoeld in het eerste lid onmiddellijk mee te delen. De directeur motiveert zijn verzoek inzake de noodzaak om de persoonsgegevens en de inlichtingen onmiddellijk toe te sturen.
	Onverminderd de verplichtingen opgenomen in de internationale instrumenten die hen binden, zijn de ondersteunende diensten verplicht om ambtshalve of op verzoek van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en de inlichtingen waarover zij beschikken in het kader van hun wettelijke opdrachten en die relevant blijkt met het oog op de verwezenlijking van de doelstellingen van de dreigingsanalyse als bedoeld in artikel 9, §2, van de wet van … betreffende de weerbaarheid van kritieke entiteiten, te communiceren.
§ 2. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Vast Comité van Toezicht op de politiediensten en van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, de nadere regels betreffende de toegang, de communicatie en het wissen van de persoonsgegevens en van de inlichtingen bedoeld in paragraaf 1.	§ 2. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Vast Comité van Toezicht op de politiediensten en van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, de nadere regels betreffende de toegang, de communicatie en het wissen van de persoonsgegevens en van de inlichtingen bedoeld in paragraaf 1.

Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Art. 3	Art. 3
§ 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 is deze wet van toepassing op publieke of private entiteiten van een in bijlage I of II bedoelde soort die:	§ 1. Binnen de grenzen van artikel 4 en onverminderd artikel 6 is deze wet van toepassing op publieke of private entiteiten van een in bijlage I of II bedoelde soort die:
1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of	1° een middelgrote onderneming zijn krachtens artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG; of
2° een onderneming die de plafonds overschrijdt zoals bepaald in lid 1 van hetzelfde artikel van deze bijlage.	2° een onderneming die de plafonds overschrijdt zoals bepaald in lid 1 van hetzelfde artikel van deze bijlage.
Artikel 3, lid 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.	Artikel 3, lid 4, van de bijlage bij Aanbeveling nr. 2003/361/EG geldt niet voor de toepassing van deze wet.
§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling nr. 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die zij verleent.	§ 2. In het kader van de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling nr. 2003/361/EG houdt de nationale cyberbeveiligingsautoriteit rekening met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen, meer bepaald wat de netwerk- en informatiesystemen betreft waarvan zij gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die zij verleent.
Op basis van het eerste lid beschouwt de nationale cyberbeveiligingsautoriteit een dergelijke entiteit als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.	Op basis van het eerste lid beschouwt de nationale cyberbeveiligingsautoriteit een dergelijke entiteit als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens.
De Koning kan de criteria bepalen op basis waarvan de mate van onafhankelijkheid van een	De Koning kan de criteria bepalen op basis waarvan de mate van onafhankelijkheid van een

entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen wordt beoordeeld.	entiteit ten opzichte van haar partnerondernemingen of verbonden ondernemingen wordt beoordeeld.
§ 3. Onverminderd artikel 6 is deze wet ook van toepassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen:	§ 3. Onverminderd artikel 6 is deze wet ook van toepassing op entiteiten van een in bijlage I of II bedoelde soort, ongeacht hun omvang, in een van de volgende gevallen:
1° de diensten worden verleend door:	1° de diensten worden verleend door:
a) aanbieders van openbare elektronische communicatienetwerken of van openbare elektronische-communicatiediensten;	a) aanbieders van openbare elektronische communicatienetwerken of van openbare elektronische-communicatiediensten;
b) verleners van vertrouwensdiensten;	b) verleners van vertrouwensdiensten;
c) registers voor topleveldomeinnamen en domeinnaamsysteem-dienstverleners;	c) registers voor topleveldomeinnamen en domeinnaamsysteem-dienstverleners;
2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;	2° de entiteit wordt geïdentificeerd als een essentiële of belangrijke entiteit overeenkomstig hoofdstuk 4 van deze titel;
3° de entiteit is een overheidsinstantie:	3° de entiteit is een overheidsinstantie:
a) die van de Federale Staat afhangt;	a) die van de Federale Staat afhangt;
b) die van de deelgebieden afhangt, geïdentificeerd overeenkomstig artikel 11, § 2;	b) die van de deelgebieden afhangt, geïdentificeerd overeenkomstig artikel 11, § 2;
c) die een hulpverleningszone is in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp in de zin van de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.	c) die een hulpverleningszone is in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp in de zin van de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.
§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.	§ 4. Onverminderd artikel 6 is deze wet van toepassing op entiteiten, ongeacht hun omvang, die worden geïdentificeerd **als kritieke entiteiten als bedoeld in de wet van ... betreffende de weerbaarheid van kritieke entiteiten.**
§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.	§ 5. Deze wet is van toepassing op entiteiten, ongeacht hun omvang, die domeinnaamregistratiediensten verlenen.

§ 6. Na raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren en/of deelsectoren toevoegen aan bijlage I of II of de bestaande sectoren en/of deelsectoren uitbreiden.	§ 6. Na raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren en/of deelsectoren toevoegen aan bijlage I of II of de bestaande sectoren en/of deelsectoren uitbreiden.
Art. 8	Art. 8
Voor de toepassing van deze wet moet worden verstaan onder:	Voor de toepassing van deze wet moet worden verstaan onder:
1° “netwerk- en informatiesysteem”:	1° “netwerk- en informatiesysteem”:
a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of	b) elk apparaat of elke groep van onderling verbonden of bij elkaar behorende apparaten, waarvan er een of meer, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken; of
c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;	c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;
2° “beveiliging van netwerk- en informatiesystemen”: het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;	2° “beveiliging van netwerk- en informatiesystemen”: het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;
3° “cyberbeveiliging”: cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de	3° “cyberbeveiliging”: cyberbeveiliging als bedoeld in artikel 2, 1), van Verordening (EU) 2019/881 van het Europees Parlement en de

Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), hierna de "cyberbeveiligingsverordening" genoemd;	Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening), hierna de "cyberbeveiligingsverordening" genoemd;
4° "nationale cyberbeveiligingsstrategie": een samenhangend kader met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en governance om die doelstellingen en prioriteiten in België te verwezenlijken;	4° "nationale cyberbeveiligingsstrategie": een samenhangend kader met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en governance om die doelstellingen en prioriteiten in België te verwezenlijken;
5° "incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;	5° "incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;
6° "bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;	6° "bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;
7° "grootschalig cyberbeveiligingsincident": een incident dat leidt tot een verstoringsniveau dat te groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie;	7° "grootschalig cyberbeveiligingsincident": een incident dat leidt tot een verstoringsniveau dat te groot is om door een getroffen lidstaat van de Europese Unie alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten van de Europese Unie;
8° "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;	8° "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;
9° "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat een dergelijk incident zich voordoet;	9° "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat een dergelijk incident zich voordoet;

10° “cyberdreiging”: een cyberdreiging bedoeld in artikel 2, punt 8), van de cyberbeveiligingsverordening;	10° “cyberdreiging”: een cyberdreiging bedoeld in artikel 2, punt 8), van de cyberbeveiligingsverordening;
11° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;	11° “significante cyberdreiging”: een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;
12° “ICT-product”: een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;	12° “ICT-product”: een ICT-product als bedoeld in artikel 2, 12), van de cyberbeveiligingsverordening;
13° “ICT-dienst”: een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;	13° “ICT-dienst”: een ICT-dienst als bedoeld in artikel 2, 13), van de cyberbeveiligingsverordening;
14° “ICT-proces”: een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;	14° “ICT-proces”: een ICT-proces als bedoeld in artikel 2, 14), van de cyberbeveiligingsverordening;
15° “kwetsbaarheid”: een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;	15° “kwetsbaarheid”: een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;
16° “norm”: een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad, hierna “Verordening (EU) nr. 1025/2012”;	16° “norm”: een norm als bedoeld in artikel 2, 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad, hierna “Verordening (EU) nr. 1025/2012”;
17° “internetknooppunt”: een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor	17° “internetknooppunt”: een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor

autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;	autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;
18° “domeinnaamsysteem” of “DNS”: een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;	18° “domeinnaamsysteem” of “DNS”: een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;
19° “DNS-dienstverlener”: een entiteit die de volgende diensten verleent:	19° “DNS-dienstverlener”: een entiteit die de volgende diensten verleent:
a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers; of b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers;	a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers; of b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers;
20° “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;	20° “register voor topleveldomeinnamen”: een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;
21° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;	21° “entiteit die domeinnaamregistratiediensten aanbiedt”: een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

22° “digitale dienst”: een dienst in de zin van artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;	22° “digitale dienst”: een dienst in de zin van artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;
23° “vertrouwensdienst”: een vertrouwensdienst in de zin van artikel 3, 16, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna de “eIDAS-verordening” genoemd;	23° “vertrouwensdienst”: een vertrouwensdienst in de zin van artikel 3, 16, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna de “eIDAS-verordening” genoemd;
24° “verlener van vertrouwensdiensten”: een verlener van vertrouwensdiensten in de zin van artikel 3, 19, van de eIDAS-verordening;	24° “verlener van vertrouwensdiensten”: een verlener van vertrouwensdiensten in de zin van artikel 3, 19, van de eIDAS-verordening;
25° “gekwalificeerde vertrouwensdienst”: een gekwalificeerde vertrouwensdienst in de zin van artikel 3, 17, van de eIDAS-verordening;	25° “gekwalificeerde vertrouwensdienst”: een gekwalificeerde vertrouwensdienst in de zin van artikel 3, 17, van de eIDAS-verordening;
26°”gekwalificeerde verlener van vertrouwensdiensten”: een gekwalificeerde verlener van vertrouwensdiensten in de zin van artikel 3, 20, van de eIDAS-verordening;	26°”gekwalificeerde verlener van vertrouwensdiensten”: een gekwalificeerde verlener van vertrouwensdiensten in de zin van artikel 3, 20, van de eIDAS-verordening;
27° “onlinemarktplaats”: een onlinemarktplaats in de zin van artikel I.8, 41°, van het Wetboek van economisch recht;	27° “onlinemarktplaats”: een onlinemarktplaats in de zin van artikel I.8, 41°, van het Wetboek van economisch recht;
28° “onlinezoekmachine”: een onlinezoekmachine als bedoeld in artikel 2, 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten;	28° “onlinezoekmachine”: een onlinezoekmachine als bedoeld in artikel 2, 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten;
29° “cloudcomputingdienst”: een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;	29° “cloudcomputingdienst”: een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;
30° “datacentrumdienst”: een dienst die structuren of groepen van structuren omvat die	30° “datacentrumdienst”: een dienst die structuren of groepen van structuren omvat die

bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT- en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole;	bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT- en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole;
31° “netwerk voor de levering van inhoud”: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;	31° “netwerk voor de levering van inhoud”: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;
32° “platform voor socialenetwerkdiensten”: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video’s en aanbevelingen	32° “platform voor socialenetwerkdiensten”: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video’s en aanbevelingen;
33° “vertegenwoordiger”: een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet;	33° “vertegenwoordiger”: een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet;
34° “overheidsinstantie”: een administratieve overheid bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:	34° “overheidsinstantie”: een administratieve overheid bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:
a) zij is niet van industriële of commerciële aard;	a) zij is niet van industriële of commerciële aard;
b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een	b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een

andere sector of deelsector van een van de bijlagen; c) zij is geen privaatrechtelijke rechtspersoon.	andere sector of deelsector van een van de bijlagen; c) zij is geen privaatrechtelijke rechtspersoon.
35° "openbaar elektronische-communicatienetwerk": een openbaar elektronische-communicatienetwerk als bedoeld in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	35° "openbaar elektronische-communicatienetwerk": een openbaar elektronische-communicatienetwerk als bedoeld in artikel 2, 10°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
36° "elektronische-communicatiedienst": een elektronische-communicatiedienst in de zin van artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	36° "elektronische-communicatiedienst": een elektronische-communicatiedienst in de zin van artikel 2, 5°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
37° "entiteit": een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;	37° "entiteit": een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;
38° "aanbieder van beheerde diensten": een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de klanten ter plaatse of op afstand;	38° "aanbieder van beheerde diensten": een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de klanten ter plaatse of op afstand;
39° "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;	39° "aanbieder van beheerde beveiligingsdiensten": een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;
40° "onderzoeksorganisatie": een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;	40° "onderzoeksorganisatie": een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen;
41° "Aanbeveling nr. 2003/361/EG": de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen;	41° "Aanbeveling nr. 2003/361/EG": de Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen;

42° “wet van 13 juni 2005”: de wet van 13 juni 2005 betreffende de elektronische communicatie;	42° “wet van 13 juni 2005”: de wet van 13 juni 2005 betreffende de elektronische communicatie;
43° “wet van 1 juli 2011”: de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	43° **wet van …: de wet van [...] betreffende de weerbaarheid van kritieke entiteiten;**
44° “koninklijk besluit van 18 april 1988”: het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering;	44° “koninklijk besluit van 18 april 1988”: het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering;
45° “nationale cyberbeveiligingsautoriteit”: de autoriteit bedoeld in artikel 16;	45° “nationale cyberbeveiligingsautoriteit”: de autoriteit bedoeld in artikel 16;
46° “nationaal CSIRT”: het nationale computer security incident response team;	46° “nationaal CSIRT”: het nationale computer security incident response team;
47° “Enisa”: het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;	47° “Enisa”: het Agentschap van de Europese Unie voor cyberbeveiliging opgericht bij de cyberbeveiligingsverordening;
48° “NCCN”: het Centrum opgericht door het koninklijk besluit van 18 april 1988;	48° “NCCN”: het Centrum opgericht door het koninklijk besluit van 18 april 1988;
49° “Verordening (EU) 2016/679”: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);	49° “Verordening (EU) 2016/679”: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
50° “gegevensbeschermingsautoriteit”: toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;	50° “gegevensbeschermingsautoriteit”: toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening (EU) 2016/679;
51° “nationale accreditatie-instantie”: de instantie bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, hierna “Verordening (EG) nr. 765/2008”;	51° “nationale accreditatie-instantie”: de instantie bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, hierna “Verordening (EG) nr. 765/2008”;
52° “beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”)”: het beleid	52° “beveiligingsbeleid voor de netwerk- en informatiesystemen (“I.B.B.”)”: het beleid

vastgelegd in een document bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen door een essentiële of belangrijke entiteit;	vastgelegd in een document bedoeld in artikel 30, met de te nemen maatregelen voor de beveiliging van netwerk- en informatiesystemen door een essentiële of belangrijke entiteit;
53° "conformiteitsbeoordelingsinstantie": de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;	53° "conformiteitsbeoordelingsinstantie": de instantie bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;
54° "sectorale overheid": de overheid bedoeld in artikel 15, § 2;	54° "sectorale overheid": de overheid bedoeld in artikel 15, § 2;
55° "CSIRT-netwerk": het netwerk van nationale CSIRT's opgericht bij artikel 15 van de NIS2-richtlijn;	55° "CSIRT-netwerk": het netwerk van nationale CSIRT's opgericht bij artikel 15 van de NIS2-richtlijn;
56° "samenwerkingsgroep": de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;	56° "samenwerkingsgroep": de samenwerkingsgroep opgericht bij artikel 14 van de NIS2-richtlijn;
57° "significant incident": elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:	57° "significant incident": elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:
1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of	1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of
2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.	2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.
58° "cybercrisis": elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:	58° "cybercrisis": elk cyberbeveiligingsincident dat wegens zijn aard of gevolgen:
1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;	1° de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;
2° een dringende besluitvorming vereist;	2° een dringende besluitvorming vereist;
3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt.	3° en de gecoördineerde inzet van verscheidene departementen en organismen vergt.
59° "Instituut": het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de	59° "Instituut": het Belgisch Instituut voor postdiensten en telecommunicatie zoals bedoeld in artikel 13 van de wet van 17 januari 2003 met betrekking tot het statuut van de

regulator van de Belgische post- en telecommunicatiesector.	regulator van de Belgische post- en telecommunicatiesector.
Art. 15	Art. 15
§ 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.	§ 1. De Koning wijst de nationale cyberbeveiligingsautoriteit aan.
§ 2. Na advies van de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een sectorale overheid en, in voorkomend geval, een sectorale inspectiedienst aanwijzen die voor een specifieke sector of deelsector belast is met het toezicht op de uitvoering van de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33.	§ 2. Na advies van de nationale cyberbeveiligingsautoriteit kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, een sectorale overheid en, in voorkomend geval, een sectorale inspectiedienst aanwijzen die voor een specifieke sector of deelsector belast is met het toezicht op de uitvoering van de bijkomende sectorale of deelsectorale maatregelen voor het beheer van cyberbeveiligingsrisico's bedoeld in artikel 33.
In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van de in het kader van de wet van 1 juli 2011 aangewezen sectorale overheden en sectorale inspectiediensten.	In het kader van de aanwijzing bedoeld in het eerste lid houdt de Koning rekening met de identiteit van de in het kader van de **wet van …** aangewezen sectorale overheden en sectorale inspectiediensten.
De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.	De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.
In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.	In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden en sectorale inspectiediensten aan.
Art. 25	Art. 25
§ 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.	§ 1. De autoriteiten bedoeld in hoofdstuk 1 van deze titel werken samen om de in deze wet vastgestelde verplichtingen na te komen.
§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening	§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening

(EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de wet van 1 juli 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten.	(EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de **wet van …** bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten.
§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.	§ 3. De essentiële en belangrijke entiteiten en de autoriteiten bedoeld in hoofdstuk 1 van deze titel werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen.
§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de wet van 1 juli 2011 bevoegde autoriteiten werken samen en wisselen regelmatig informatie uit inzake het als kritiek aanmerken van infrastructuren, over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.	§ 4. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de in het kader van de **wet van …** bevoegde autoriteiten werken samen en wisselen regelmatig informatie uit inzake het als kritiek aanmerken van infrastructuren, over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor **kritieke entiteiten als bedoeld in de wet van …** zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen.
§ 5. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de autoriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende	§ 5. De in hoofdstuk 1 van deze titel bedoelde autoriteiten en de autoriteiten die bevoegd zijn krachtens Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende

digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 en de wet van 13 juni 2005, wisselen regelmatig relevante informatie uit, onder meer met betrekking tot relevante incidenten en cyberdreigingen.	digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 en de wet van 13 juni 2005, wisselen regelmatig relevante informatie uit, onder meer met betrekking tot relevante incidenten en cyberdreigingen.
§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform op dat de in artikel 15 bedoelde autoriteiten en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van deze wet op elkaar af te stemmen.	§ 6. De nationale cyberbeveiligingsautoriteit richt een coördinatie- en evaluatieplatform op dat de in artikel 15 bedoelde autoriteiten en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van deze wet op elkaar af te stemmen.
Art. 28	Art. 28
§ 1. De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de vijf jaar bij op basis van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN en, in voorkomend geval, de gegevensbeschermingsautoriteiten.	§ 1. De in Raad vergaderde ministers keuren de nationale cyberbeveiligingsstrategie goed en werken deze minstens om de vijf jaar bij op basis van prestatie-indicatoren, na advies van de Nationale Veiligheidsraad, de in artikel 15 bedoelde autoriteiten, het NCCN en, in voorkomend geval, de gegevensbeschermingsautoriteiten.
Deze strategie bepaalt de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.	Deze strategie bepaalt de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.
§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:	§ 2. De nationale cyberbeveiligingsstrategie omvat onder meer:
1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;	1° de doelstellingen en prioriteiten van de nationale cyberbeveiligingsstrategie, met name inzake de in de bijlagen I en II bedoelde sectoren;
2° een governancekader om de in punt 1° bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van de taken en verantwoordelijkheden van de overheid en de andere belanghebbenden alsook van het in paragraaf 3 bedoelde beleid;	2° een governancekader om de in punt 1° bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van de taken en verantwoordelijkheden van de overheid en de andere belanghebbenden alsook van het in paragraaf 3 bedoelde beleid;
3° een governancekader dat de taken en verantwoordelijkheden van de belanghebbenden in België verduidelijkt, ter	3° een governancekader dat de taken en verantwoordelijkheden van de belanghebbenden in België verduidelijkt, ter

onderbouwing van de samenwerking en coördinatie, in België, tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel, alsook van de samenwerking en coördinatie tussen die autoriteiten en uit hoofde van sectorspecifieke rechtsinstrumenten van de Europese Unie bevoegde autoriteiten;	onderbouwing van de samenwerking en coördinatie, in België, tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel, alsook van de samenwerking en coördinatie tussen die autoriteiten en uit hoofde van sectorspecifieke rechtsinstrumenten van de Europese Unie bevoegde autoriteiten;
4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;	4° een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in België;
5° een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de private sector;	5° een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de private sector;
6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;	6° een lijst van de verschillende belanghebbenden en autoriteiten die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;
7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;	7° een beleidskader voor versterkte coördinatie tussen de autoriteiten bedoeld in hoofdstuk 1 van deze titel en de uit hoofde van de **wet van …** bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;
8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;	8° een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren;
9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;	9° een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale cyberbeveiligingsstrategie;
10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.	10° een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale cyberbeveiligingsstrategie.
§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale cyberbeveiligingsstrategie:	§ 3. Er worden beleidsmaatregelen genomen die integraal deel uitmaken van de nationale cyberbeveiligingsstrategie:
1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-	1° inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-

diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;	diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;
2° inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;	2° inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;
3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 22;	3° voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden overeenkomstig artikel 22;
4° inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;	4° inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;
5° voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;	5° voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;
6° voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligingsvaardigheden, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiëne, gericht op burgers, belanghebbenden en entiteiten;	6° voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligingsvaardigheden, bewustmakings- en onderzoeks- en ontwikkelingsinitiatieven rond cyberbeveiliging, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiëne, gericht op burgers, belanghebbenden en entiteiten;
7° voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;	7° voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;
8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillig delen van cyberbeveiligingsinformatie tussen entiteiten;	8° met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillig delen van cyberbeveiligingsinformatie tussen entiteiten;

9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiëne van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze wet zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;	9° voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiëne van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze wet zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;
10° voor het bevorderen van actieve cyberbescherming.	10° voor het bevorderen van actieve cyberbescherming.
Art. 37	Art. 37
§ 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig artikel 35 is ontvangen. Daarbij beschermt het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie.	§ 1. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het nationale CSIRT de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig artikel 35 is ontvangen. Daarbij beschermt het nationale CSIRT, overeenkomstig het Unie- of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsook de vertrouwelijkheid van de verstrekte informatie.
§ 2. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entiteit, het NCCN, de eventuele betrokken sectorale overheid en de betrokken minister, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.	§ 2. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kan het nationale CSIRT, na raadpleging van de betrokken entiteit, het NCCN, de eventuele betrokken sectorale overheid en de betrokken minister, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.
§ 3. De nationale cyberbeveiligingsautoriteit stuurt, op verzoek van de eventuele betrokken sectorale overheid, de op grond van artikel 34, § 1, eerste lid, ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.	§ 3. De nationale cyberbeveiligingsautoriteit stuurt, op verzoek van de eventuele betrokken sectorale overheid, de op grond van artikel 34, § 1, eerste lid, ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.
§ 4. De nationale cyberbeveiligingsautoriteit dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en	§ 4. De nationale cyberbeveiligingsautoriteit dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en

bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld.	bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld.
§ 5. Het nationale CSIRT verstrekt de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld door exploitanten van infrastructuren die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuren zijn geïdentificeerd.	§ 5. Het nationale CSIRT verstrekt de uit hoofde van de **wet van …** bevoegde autoriteiten informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig artikel 34, § 1, eerste lid, en artikel 38, § 1, zijn gemeld **door kritieke entiteiten als bedoeld in de wet van ….**
Art. 40	Art. 40
§ 1. De in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling wordt verricht door een conformiteitsbeoordelingsinstantie die erkend is door de nationale cyberbeveiligingsautoriteit volgens de door de Koning bepaalde voorwaarden.	§ 1. De in artikel 39, eerste lid, 1°, bedoelde regelmatige conformiteitsbeoordeling wordt verricht door een conformiteitsbeoordelingsinstantie die erkend is door de nationale cyberbeveiligingsautoriteit volgens de door de Koning bepaalde voorwaarden.
Voor het toezicht op entiteiten die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.	Voor het toezicht op entiteiten die worden geïdentificeerd **als kritieke entiteiten als bedoeld in de wet van …** en overheidsinstanties beschikken de conformiteitsbeoordelingsinstantie en de natuurlijke personen die de conformiteit beoordelen over een veiligheidsmachtiging.
§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit kan op elk ogenblik nagaan of de conformiteitsbeoordelingsinstanties de in paragraaf 1 bedoelde erkenningsvoorwaarden naleven, overeenkomstig de bepalingen van dit hoofdstuk.	§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit kan op elk ogenblik nagaan of de conformiteitsbeoordelingsinstanties de in paragraaf 1 bedoelde erkenningsvoorwaarden naleven, overeenkomstig de bepalingen van dit hoofdstuk.
Art. 45	Art. 45
§ 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de wet van 1 juli 2011 de bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een exploitant van een infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur wordt geïdentificeerd, voldoet aan deze wet. In	§ 1. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen de uit hoofde van de **wet van …** de bevoegde autoriteiten in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen **dat een kritieke entiteit als bedoeld in de wet van …,** voldoet aan deze wet. In voorkomend geval kunnen de uit hoofde van de **wet van …** bevoegde autoriteiten de

voorkomend geval kunnen de uit hoofde van de wet van 1 juli 2011 bevoegde autoriteiten de inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een exploitant van een infrastructuur die is geïdentificeerd als kritieke infrastructuur uit hoofde van de wet van 1 juli 2011.	inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van **een kritieke entiteit als bedoeld in de zin van de wet van ….**
§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst werken samen met de relevante autoriteiten die bevoegd zijn uit hoofde van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen met name het oversightforum dat is opgericht op grond van artikel 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële of belangrijke entiteit die op grond van artikel 31 van bovengenoemde verordening als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze wet.	§ 2. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst werken samen met de relevante autoriteiten die bevoegd zijn uit hoofde van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011. De inspectiedienst van de nationale cyberbeveiligingsautoriteit en de eventuele bevoegde sectorale overheid of sectorale inspectiedienst stellen met name het oversightforum dat is opgericht op grond van artikel 32, lid 1, van bovengenoemde verordening in kennis wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële of belangrijke entiteit die op grond van artikel 31 van bovengenoemde verordening als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze wet.
Art. 67	Art. 67
De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:	De verwerking van persoonsgegevens vindt plaats voor de volgende doeleinden:
1° de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;	1° de verbetering van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;
2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren	2° de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit, met name het identificeren van de entiteiten, het informeren

en sensibiliseren van de gebruikers van informatie- en communicatiesystemen, het toekennen van subsidies, de internationale samenwerking tussen de nationale cyberbeveiligingsautoriteit, de bevoegde autoriteiten van andere lidstaten, internationale fora voor cyberbeveiliging, Enisa en de Europese Commissie;	en sensibiliseren van de gebruikers van informatie- en communicatiesystemen, het toekennen van subsidies, de internationale samenwerking tussen de nationale cyberbeveiligingsautoriteit, de bevoegde autoriteiten van andere lidstaten, internationale fora voor cyberbeveiliging, Enisa en de Europese Commissie;
3° het beheer van cybercrises en cyberbeveiligingsincidenten;	3° het beheer van cybercrises en cyberbeveiligingsincidenten;
4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikelen: a) 19, § 1; b) 21, § 2, tweede lid, 1° tot 3°; c) 22, §§ 2 tot 6; d) 37, §§ 1 tot 3 en § 5;	4° de uitvoering van de taken van het nationale CSIRT bedoeld in de volgende artikel en: a) 19, § 1; b) 21, § 2, tweede lid, 1° tot 3°; c) 22, §§ 2 tot 6; d) 37, §§ 1 tot 3 en § 5;
5° de samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de wet van 1 juli 2011, alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en de wet van 1 juli 2011;	5° de samenwerking, met name de informatie-uitwisseling tussen de nationale cyberbeveiligingsautoriteit, de eventuele sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de **wet van …,** alsook de autoriteiten bedoeld in artikel 25, § 2, in het kader van de uitvoering van deze wet en **de wet van …;**
6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;	6° de samenwerking tussen essentiële en belangrijke entiteiten en de autoriteiten bedoeld in titel 2, hoofdstuk 1;
7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;	7° het delen van informatie tussen de autoriteiten bedoeld in artikel 25, § 5;
8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;	8° de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten;
9° het melden van incidenten en bijna-incidenten;	9° het melden van incidenten en bijna-incidenten;
10° de controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes.	10° de controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes.

Art. 68	Art. 68
De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:	De verwerkingsverantwoordelijken verwerken de volgende categorieën van persoonsgegevens:
1° voor het doeleinde bedoeld in artikel 67, 1°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen bedoeld in artikel 67, 1°;	1° voor het doeleinde bedoeld in artikel 67, 1°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de opdrachten rond de verbetering van de cyberbeveiliging, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen bedoeld in artikel 67, 1°;
2° voor het doeleinde bedoeld in artikel 67, 2°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit;	2° voor het doeleinde bedoeld in artikel 67, 2°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van de nationale cyberbeveiligingsautoriteit;
3° voor het doeleinde bedoeld in artikel 67, 3°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij cybercrises en cyberbeveiligingsincidenten;	3° voor het doeleinde bedoeld in artikel 67, 3°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij cybercrises en cyberbeveiligingsincidenten;
4° voor het doeleinde bedoeld in artikel 67, 4°: de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, en elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van voornoemde wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT;	4° voor het doeleinde bedoeld in artikel 67, 4°: de identificatie-, verbindings-, locatie-, elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, en elektronische-communicatiemetagegevens als bedoeld in artikel 2, 93°, van voornoemde wet van 13 juni 2005, van de personen die betrokken zijn bij de uitvoering van de taken van het CSIRT;
5° voor het doeleinde bedoeld in artikel 67, 5°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking in het kader van de wet van 1 juli 2011;	5° voor het doeleinde bedoeld in artikel 67, 5°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking in het kader van **de wet van …;**
6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;	6° voor het doeleinde bedoeld in artikel 67, 6°: de identificatiegegevens van de personen die betrokken zijn bij de samenwerking;

7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;	7° voor het doeleinde bedoeld in artikel 67, 7°: de identificatiegegevens van de personen die betrokken zijn bij het delen van informatie;
8° voor het doeleinde bedoeld in artikel 67, 8°: de identificatiegegevens van de personen die betrokken zijn bij het waarborgen van de continuïteit van de dienstverlening;	8° voor het doeleinde bedoeld in artikel 67, 8°: de identificatiegegevens van de personen die betrokken zijn bij het waarborgen van de continuïteit van de dienstverlening;
9° voor het doeleinde bedoeld in artikel 67, 9°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de melding;	9° voor het doeleinde bedoeld in artikel 67, 9°: de identificatie-, verbindings-, locatie- en elektronische- communicatiegegevens als bedoeld in artikel 2, 91°, van de wet van 13 juni 2005, van de personen die betrokken zijn bij de melding;
10° voor het doeleinde bedoeld in artikel 67, 10°: de persoonsgegevens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controles, dit toezicht of deze sancties.	10° voor het doeleinde bedoeld in artikel 67, 10°: de persoonsgegevens die nodig en relevant zijn voor de uitoefening van de controle-, toezichts- en sanctieopdrachten, van de personen die betrokken zijn bij deze controles, dit toezicht of deze sancties.

COORDINATION DES ARTICLES

Texte de base	**Texte adapté au projet de loi**
Loi du 13 juin 2005 relative aux communications électroniques	
Art. 28/3	Art. 28/3
§ 1er. Toute entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques, en réponse à une demande écrite formulée par une autre entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques, fait droit à toute demande raisonnable d'accès à ses infrastructures passives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.	§ 1er. Toute entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques, en réponse à une demande écrite formulée par une autre entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques, fait droit à toute demande raisonnable d'accès à ses infrastructures passives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.
§ 2. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:	§ 2. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:
1° la capacité technique de l'infrastructure passive à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 1er;	1° la capacité technique de l'infrastructure passive à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 1er;
2° l'espace disponible pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 1er, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques pour autant que ceux-ci aient été démontrés de manière suffisante;	2° l'espace disponible pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 1er, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques pour autant que ceux-ci aient été démontrés de manière suffisante;
3° des considérations de sûreté et de santé publique;	3° des considérations de sûreté et de santé publique;
4° l'intégrité et la sécurité de l'infrastructure passive, en particulier de celle constituant une infrastructure critique nationale visée par la loi	4° l'intégrité et la sécurité de l'infrastructure passive, en particulier de celle constituant une infrastructure critique nationale visée **par la loi**

du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	**du … relative à la résilience des entités critiques**;
5° le risque d'interférence grave entre les services de communications électroniques en projet et ceux fournis à l'aide des infrastructures passives;	5° le risque d'interférence grave entre les services de communications électroniques en projet et ceux fournis à l'aide des infrastructures passives;
6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure passive, offerts par l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.	6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure passive, offerts par l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.
L'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques indique les raisons de son refus dans un délai de deux mois à compter de la date de réception de la demande d'accès complète.	L'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques indique les raisons de son refus dans un délai de deux mois à compter de la date de réception de la demande d'accès complète.
§ 3. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'Institut, conformément à l'article 4 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges.	§ 3. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'Institut, conformément à l'article 4 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges.
§ 4. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure passive lorsque l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques n'est pas la propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques d'obtenir les permis et autorisations requis pour	§ 4. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure passive lorsque l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques n'est pas la propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux publics de communications électroniques d'obtenir les permis et autorisations requis pour

la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.	la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.
Art. 105	Art. 105
§ 1er. Dans le but de préserver les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l'alinéa 3, 1°, avant d'utiliser un élément de leur réseau 5G.	§ 1er. Dans le but de préserver les intérêts visés à l'article 3, § 1er, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, les MNO obtiennent une autorisation établie de façon conjointe par les ministres concernés visés à l'alinéa 3, 1°, avant d'utiliser un élément de leur réseau 5G.
En tenant compte des intérêts visés à l'alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d'incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu'ils ne puissent bénéficier de certains de ces services.	En tenant compte des intérêts visés à l'alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut prévoir que cette autorisation est également nécessaire avant que les MNO ne puissent bénéficier de services de fournisseurs qui consistent à intervenir ponctuellement dans la gestion de ce réseau, notamment en cas d'incident ou de modification majeure du réseau, ou à gérer ou superviser quotidiennement des éléments du réseau ou est également nécessaire avant qu'ils ne puissent bénéficier de certains de ces services.
Pour l'application du présent article, on entend par:	Pour l'application du présent article, on entend par:
1° ministres concernés: le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères;	1° ministres concernés: le Premier ministre, le ministre des Télécommunications, le ministre de la Défense, le ministre de la Justice, le ministre de l'Intérieur et le ministre des Affaires étrangères;
2° réseau 5G: un réseau de communications électroniques dont le réseau d'accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications.	2° réseau 5G: un réseau de communications électroniques dont le réseau d'accès radioélectrique est basé sur une interface radio spécifiée dans la recommandation UIT-R M.2150 de l'Union internationale des télécommunications.
Les alinéas 1er et 2 ne sont pas d'application:	Les alinéas 1er et 2 ne sont pas d'application:
1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie;	1° pour l'utilisation d'éléments passifs du réseau, à savoir des éléments qui ne sont pas alimentés par une source d'énergie;
2° pour les points de terminaison pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la	2° pour les points de terminaison pour autant qu'ils ne contiennent pas une partie radio basée sur une interface radio spécifiée dans la

recommandation UIT-R M.2150 de l'Union internationale des télécommunications;	recommandation UIT-R M.2150 de l'Union internationale des télécommunications;
3° pour les éléments de réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture d'un réseau 5G.	3° pour les éléments de réseaux mobiles de quatrième génération et des générations antérieures, pour autant qu'ils ne soient pas nécessaires à la fourniture d'un réseau 5G.
Si l'utilisation de l'élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.	Si l'utilisation de l'élément de réseau ou le recours au fournisseur de services est déjà effectif à la date d'entrée en vigueur de l'arrêté royal visé au paragraphe 4, alinéa 1er, une autorisation de régularisation est demandée dans les deux mois qui suivent cette date.
§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres:	§ 2. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, le Roi peut, par arrêté délibéré en Conseil des ministres:
1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO;	1° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à une ou plusieurs catégories de MVNO;
2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public ASTRID, et aux exploitants d'un réseau privé de communications électroniques qui ont été désignés comme exploitant d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	2° étendre l'obligation d'obtenir les autorisations visées au paragraphe 1er à la société anonyme de droit public ASTRID, et aux exploitants d'un réseau privé de communications électroniques qui ont été désignés comme **entité critique au sens de la loi … relative à la résilience des entités critiques;**
3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres exploitants d'un réseau privé de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er;	3° charger une ou plusieurs autorités de désigner par décision individuelle, lorsque c'est nécessaire pour préserver les intérêts visés au paragraphe 1er, alinéa 1er, les autres exploitants d'un réseau privé de communications électroniques soumis à l'obligation d'obtenir les autorisations visées au paragraphe 1er;
4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er, alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau;	4° préciser les hypothèses dans lesquelles une autorisation visée au paragraphe 1er, alinéa 1er, est nécessaire en cas de mise à jour d'un logiciel ou d'un dispositif matériel du réseau;
§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.	§ 3. Le demandeur introduit son dossier auprès de l'Institut, selon les modalités qu'il fixe sur son site internet.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, les modalités de traitement de la demande et la composition du dossier.	Le Roi fixe, par arrêté délibéré en Conseil des ministres, les modalités de traitement de la demande et la composition du dossier.
Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.	Les ministres concernés, l'Institut et les services de renseignement et de sécurité peuvent demander des informations ou des documents complémentaires au demandeur ou à toute personne pouvant contribuer utilement à leur information.
§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en œuvre les restrictions et délais de mise en œuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.	§ 4. Lorsqu'ils prennent leur décision après l'examen de la demande visée au paragraphe 1er, ou la revoient d'initiative en raison d'un nouvel élément de nature à remettre en cause leur décision, les ministres concernés mettent en œuvre les restrictions et délais de mise en œuvre fixés par le Roi, par arrêté délibéré en Conseil des ministres, concernant l'utilisation, sur le territoire national ou dans les zones sensibles de ce territoire, d'éléments de réseau ou de services de fournisseurs à haut risque.
Ces restrictions et ces délais de mise en œuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.	Ces restrictions et ces délais de mise en œuvre ne peuvent être fixés qu'en vue de garantir la protection des intérêts visés au paragraphe 1er, alinéa 1er.
Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en œuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.	Lorsqu'ils revoient leur décision d'initiative et lorsque c'est justifié, les ministres concernés fixent une date de mise en œuvre de la nouvelle décision qui est postérieure aux délais fixés par l'arrêté royal visé à l'alinéa 1er et qui suit d'au moins cinq ans la date de sa notification.
Le profil de risque d'un fournisseur est évalué sur base des critères suivants:	Le profil de risque d'un fournisseur est évalué sur base des critères suivants:
1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un Etat membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants:	1° la probabilité qu'il subisse une ingérence de la part d'un pays autre qu'un Etat membre de l'Union européenne, une telle ingérence pouvant être facilitée, sans s'y limiter, par la présence d'un ou de plusieurs des facteurs suivants:
a) un lien fort avec les autorités publiques du pays en question;	a) un lien fort avec les autorités publiques du pays en question;
b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des	b) la législation ou la situation au sein du pays en question, notamment lorsqu'il n'y a pas de contrôle démocratique ou législatif en place ou en l'absence de conventions de protection des

données ou de sécurité entre l'Union européenne et le pays en question;	données ou de sécurité entre l'Union européenne et le pays en question;
c) les caractéristiques de la propriété d'entreprise du fournisseur;	c) les caractéristiques de la propriété d'entreprise du fournisseur;
d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements;	d) la capacité du pays en question à exercer toute forme de pression, y compris par rapport au lieu de fabrication des équipements;
e) le fait que le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive;	e) le fait que le pays d'où est originaire le fournisseur mène ou est associé à une politique cyber offensive;
2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité;	2° la capacité du fournisseur à garantir l'approvisionnement en termes de délai et de quantité;
3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.	3° la qualité globale des produits ou services et les pratiques en matière de sécurité du fournisseur, y compris le degré de contrôle sur sa propre chaîne d'approvisionnement et la question de savoir si une hiérarchisation adéquate des priorités est donnée aux pratiques en matière de sécurité.
Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.	Le Roi peut, par arrêté délibéré en Conseil des ministres, compléter les critères visés à l'alinéa 4.
Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.	Un seul de ces critères peut justifier qu'un fournisseur soit qualifié comme étant à haut risque.
Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.	Le profil de risque d'un fournisseur est évalué sur la base d'un avis des services de renseignement et de sécurité en ce qui concerne le critère fixé à l'alinéa 4, 1°, et sur la base d'un avis de l'Institut en ce qui concerne les critères fixés à l'alinéa 4, 2° et 3°.
Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.	Les zones sensibles sont identifiées par le Roi, sur base d'un avis du Conseil national de sécurité, et ce, en tenant compte de la présence dans ces zones de sites liés aux intérêts visés au paragraphe 1er, alinéa 1er.
L'arrêté royal identifiant les zones sensibles est publié par voie de mention au *Moniteur belge*.	L'arrêté royal identifiant les zones sensibles est publié par voie de mention au *Moniteur belge*.
§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou	§ 5. Lorsque les ministres concernés entendent refuser l'autorisation, l'assortir de conditions ou

revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.	revoir leur décision, le demandeur dispose de vingt-huit jours après avoir reçu le projet de décision pour présenter ses observations écrites.
La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.	La possibilité est offerte au demandeur d'être entendu. Il peut se faire accompagner par les conseils, techniques ou juridiques, de son choix.
Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.	Les ministres concernés peuvent se faire représenter par l'administration de leur choix. L'Institut et les services de renseignement et de sécurité peuvent participer à l'audition.
§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.	§ 6. Les ministres concernés prennent ensemble une seule décision. L'Institut pose tous les actes utiles en vue de sa préparation.
Dans le délai fixé par le Roi, qui commence à partir de l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.	Dans le délai fixé par le Roi, qui commence à partir de l'introduction de la demande, le demandeur reçoit la décision des ministres qui octroie l'autorisation ou le projet de décision dans lequel ils refusent l'autorisation ou l'assortissent de conditions.
En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.	En cas d'audition ou d'observations écrites du demandeur, visées au paragraphe 5, les ministres prennent leur décision au plus tard dans le délai fixé par le Roi, qui commence à partir de la réception des observations écrites ou de la date de l'audition, la date la plus tardive étant retenue.
La demande d'informations ou de documents visée au paragraphe 3, alinéa 3, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.	La demande d'informations ou de documents visée au paragraphe 3, alinéa 3, ou adressée au demandeur afin qu'il complète son dossier, suspend les délais fixés aux alinéas 2 et 3, jusqu'au jour où les informations ou documents demandés sont fournis.
Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.	Le défaut de décision ou de projet de décision visé à l'alinéa 2 dans le délai fixé en vertu de l'alinéa 2 ou de l'alinéa 3 équivaut à un refus.
§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.	§ 7. La personne qui obtient une copie de la liste des zones sensibles visée au paragraphe 4, alinéa 8, ne peut la transmettre qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission dans le cadre du déploiement et de l'exploitation du réseau 5G.

Est punie d'une amende pénale de 1000 euros à 100 000 euros: la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.	Est punie d'une amende pénale de 1000 euros à 100 000 euros: la personne qui divulgue des informations relatives à la liste visée à l'alinéa 1er à une personne qui n'est pas visée à cet alinéa.
Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.	Les personnes qui traitent une demande d'autorisation ou la révision d'une décision antérieure peuvent communiquer à des administrations publiques qu'elles consultent dans ce cadre des informations confidentielles lorsque c'est nécessaire pour l'accomplissement de la tâche qu'elles leur confient.
Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent pas communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.	Les personnes et les administrations publiques visées à l'alinéa 3 ne peuvent pas communiquer à des tiers des informations confidentielles dont elles ont connaissance dans le cadre de l'application du présent article, hormis les exceptions prévues par la loi.
Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.	Ces informations confidentielles sont celles qui sont qualifiées comme telles par la personne qui les a fournies, sans préjudice de l'article 23, paragraphe 3, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.
La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.	La violation de l'interdiction visée à l'alinéa 4 sera punie par les peines prévues à l'article 458 du Code pénal ou l'une de ces peines.
§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des États membres de l'Union européenne. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.	§ 8. Lorsqu'un MNO offre en Belgique des services de communications électroniques à l'aide d'un réseau 5G, les infrastructures de ce réseau doivent se trouver sur le territoire des États membres de l'Union européenne. En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er, et par arrêté délibéré en Conseil des ministres, le Roi peut fixer les exigences qui découlent de cette obligation.
En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'Il détermine, au sein du territoire des États membres de l'Union européenne.	En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi impose aux MNO visés à l'alinéa 1er les règles nécessaires pour qu'ils effectuent les activités indispensables au fonctionnement, à la sécurité et à la continuité de leur réseau, qu'Il détermine, au sein du territoire des États membres de l'Union européenne.

En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et exploitants d'un réseau privé de communications électroniques qui sont soumis aux autorisations visées au paragraphe 1er.	En tenant compte des intérêts visés au paragraphe 1er, alinéa 1er et par arrêté délibéré en Conseil des ministres, le Roi peut étendre les règles et exigences visées aux alinéas 1er et 2 aux MVNO et exploitants d'un réseau privé de communications électroniques qui sont soumis aux autorisations visées au paragraphe 1er.
Art. 126/3	Art. 126/3
§ 1er. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée des:	§ 1er. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée des:
- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;	- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;
- zones de police dans lesquelles au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.	- zones de police dans lesquelles au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.
Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:	Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:
a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;	a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;
b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;	b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.	c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.
Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:	Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de:
a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;	a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;
b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;	b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;
c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.	c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.
Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.	Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.
Les statistiques relatives au nombre d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.	Les statistiques relatives au nombre d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.
Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.	Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.
Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.	Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.	La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.
Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.	Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.
Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.	Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.
Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.	Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.
§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.	§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.
Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace	Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace

informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.	informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.
L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.	L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.
§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir:	§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir:
a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;	a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;
b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;	b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;
c) les stations de métro et de pré-métro;	c) les stations de métro et de pré-métro;
d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;	d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;
e) les bâtiments affectés à l'administration des douanes et accises;	e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;	f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, c), de la loi du 5 mai 2014 relative à l'internement;
g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;	g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;
h) les établissements visés à l'article 3.1.a), de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;	h) les établissements visés à l'article 3.1.a), de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;
i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;	i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;
j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;	j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés **dans la loi du … relative à la résilience des entités critiques** et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;
k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;	k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services des entités essentielles au sens de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;	l) les systèmes de réseau et d'information qui soutiennent la fourniture des services des entités essentielles au sens de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;
m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.	m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.
§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:	§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir:
a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;	a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;
b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;	b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;
c) pour le transport, les autoroutes et les parkings publics attenants;	c) pour le transport, les autoroutes et les parkings publics attenants;
d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:	d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances:
i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution; ii) les maisons communales et les hôtels de ville;	i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution; ii) les maisons communales et les hôtels de ville;

iii) le palais royal;	iii) le palais royal;
iv) les domaines royaux;	iv) les domaines royaux;
v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;	v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;
vi) les communes dans lesquelles se trouvent des domaines militaires;	vi) les communes dans lesquelles se trouvent des domaines militaires;
vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;	vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;
e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;	e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;
f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:	f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale:
i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;	i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;
ii) la Banque nationale de Belgique;	ii) la Banque nationale de Belgique;
g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.	g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.
§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:	§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir:
a) les ambassades et les représentations diplomatiques;	a) les ambassades et les représentations diplomatiques;
b) les bâtiments affectés à l'Union européenne;	b) les bâtiments affectés à l'Union européenne;
c) les bâtiments et infrastructures affectés à l'OTAN;	c) les bâtiments et infrastructures affectés à l'OTAN;
d) les institutions de l'Espace économique européen;	d) les institutions de l'Espace économique européen;
e) les institutions des Nations Unies;	e) les institutions des Nations Unies;
f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.	f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.	§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.
Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.	Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.
Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.	Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.
A l'exception de la liste des lieux visés au paragraphe 4, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.	A l'exception de la liste des lieux visés au paragraphe 4, b), mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.
L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.	L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.
Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.	Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.
L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au *Moniteur belge*.	L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au *Moniteur belge*.
Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des	Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des

données, ainsi que leur durée de conservation, aux opérateurs.	données, ainsi que leur durée de conservation, aux opérateurs.
Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.	Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

Art. 3	Art. 3
§ 1er. La présente loi s'applique à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement sur la cybersécurité.	§ 1er. La présente loi s'applique à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement sur la cybersécurité.
§ 2. Les chapitres 1er à 4, 7 et 8, ainsi que les articles 21 et 22, s'appliquent également à une certification européenne de cybersécurité rendue obligatoire.	§ 2. Les chapitres 1er à 4, 7 et 8, ainsi que les articles 21 et 22, s'appliquent également à une certification européenne de cybersécurité rendue obligatoire.
Lors de la mise en œuvre des articles 21 et 22 dans le cadre de la certification visée à l'alinéa 1er, les articles 19 et 26 sont applicables.	Lors de la mise en œuvre des articles 21 et 22 dans le cadre de la certification visée à l'alinéa 1er, les articles 19 et 26 sont applicables.
Le Roi peut, par arrêté délibéré en Conseil des ministres, rendre applicables, en tout ou en partie, les chapitres 5 et 6 dans le cadre de la certification visée à l'alinéa 1er.	Le Roi peut, par arrêté délibéré en Conseil des ministres, rendre applicables, en tout ou en partie, les chapitres 5 et 6 dans le cadre de la certification visée à l'alinéa 1er.
§ 3. La présente loi est sans préjudice des compétences de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle dont disposent les autorités publiques, notamment les autorités de surveillance de marché ou les autorités sectorielles visées à l'article 6, 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et de l'article 2, alinéa 1er, 1°, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures	§ 3. La présente loi est sans préjudice des compétences de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle dont disposent les autorités publiques, notamment les autorités de surveillance de marché ou les autorités sectorielles visées **à l'article 3, 2°, de la loi du … relative à la résilience des entités critiques.**

critiques dans le sous-secteur du transport aérien.	
Dans le respect du paragraphe 2, les autorités visées à l'alinéa 1er et les services d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.	Dans le respect du paragraphe 2, les autorités visées à l'alinéa 1er et les services d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.
§ 4. L'article 5, § § 2 à 4, n'est applicable ni à la Banque nationale de Belgique visée à la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique ni à la FSMA visée à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ni au SPF Économie visé au Code de droit économique.	§ 4. L'article 5, § § 2 à 4, n'est applicable ni à la Banque nationale de Belgique visée à la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique ni à la FSMA visée à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ni au SPF Économie visé au Code de droit économique.
§ 5. La présente loi ne porte pas préjudice à l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.	§ 5. La présente loi ne porte pas préjudice à l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.
Art. 6	Art. 6
§ 1er. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 accomplissent leurs tâches en concertation avec les autorités publiques, notamment avec l'autorité nationale d'accréditation. En fonction de l'objet précis du schéma de certification, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 peuvent également consulter les acteurs privés concernés par la certification en matière de cybersécurité.	§ 1er. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 accomplissent leurs tâches en concertation avec les autorités publiques, notamment avec l'autorité nationale d'accréditation. En fonction de l'objet précis du schéma de certification, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 peuvent également consulter les acteurs privés concernés par la certification en matière de cybersécurité.
§ 2. Conformément à l'article 58, paragraphe 7, h), du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'une part, les autorités sectorielles et les services d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou à l'article 7, § § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes	§ 2. Conformément à l'article 58, paragraphe 7, h), du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'une part, les autorités sectorielles et les services d'inspection, visés respectivement **aux articles 3, 2° et 33 de la loi du … relative à la résilience des entités critiques ou à l'article 15, § 2, de la loi du 24 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité**

d'information d'intérêt général pour la sécurité publique, l'Institut belge des services postaux et des télécommunications et l'autorité nationale d'accréditation, d'autre part, s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, notamment en matière de délivrance de certificats, de contrôle, de sanctions et de réclamations. Lorsqu'un échange d'informations porte sur des données à caractère personnel, cet échange est effectué conformément aux dispositions du chapitre 8. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.	**publique,** l'Institut belge des services postaux et des télécommunications et l'autorité nationale d'accréditation, d'autre part, s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, notamment en matière de délivrance de certificats, de contrôle, de sanctions et de réclamations. Lorsqu'un échange d'informations porte sur des données à caractère personnel, cet échange est effectué conformément aux dispositions du chapitre 8. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.
§ 3. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 communiquent aux destinataires, à savoir une autorité sectorielle, un service d'inspection, l'inspection aéroportuaire, l'inspection aéronautique ou la Belgian Supervising Authority for Air Navigation Services visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, à l'article 7, §§ 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou aux articles 2, alinéa 1er, 1° et 9°, et 15, §§ 1er à 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, toute information obtenue dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi ou d'un schéma européen de certification de cybersécurité lorsque cette information porte sur un manquement à l'article 13 de la loi précitée du 1er juillet 2011, aux articles 20, 21, § 1er, et 33, de la loi précitée du 7 avril 2019, à l'article 11 de l'arrêté royal précité du 2 décembre 2011 ou aux sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, et que l'entité concernée par	§ 3. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 communiquent aux destinataires, à savoir une autorité sectorielle, un service d'inspection, l'inspection aéroportuaire, l'inspection aéronautique ou la Belgian Supervising Authority for Air Navigation Services visés respectivement aux **articles 3, 2° et 33 de la loi du … relative à la résilience des entités critiques, à l'article 15, § 2, de la loi du 24 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique**, toute information obtenue dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi ou d'un schéma européen de certification de cybersécurité lorsque cette information porte sur un manquement à l'article 13 de la loi précitée du 1er juillet 201, **à l'article 30 de la loi précitée du 24 avril 2024,** à l'article 11 de l'arrêté royal précité du 2 décembre 2011 ou aux sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, et que l'entité concernée par l'information se trouve sous la surveillance desdits destinataires.

l'information se trouve sous la surveillance desdits destinataires.	
§ 4. Dans le cadre de la coopération prévue aux paragraphes 2 et 3, les autorités publiques dépositaires, par état, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces informations confidentielles à l'autorité visée à l'article 5, § 1er, ou à l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.	§ 4. Dans le cadre de la coopération prévue aux paragraphes 2 et 3, les autorités publiques dépositaires, par état, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces informations confidentielles à l'autorité visée à l'article 5, § 1er, ou à l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.
Seules les informations nécessaires en matière de contrôle, de sanctions et de réclamations peuvent être communiquées. Lorsque ces informations portent sur des données à caractère personnel, le chapitre 8 est d'application. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.	Seules les informations nécessaires en matière de contrôle, de sanctions et de réclamations peuvent être communiquées. Lorsque ces informations portent sur des données à caractère personnel, le chapitre 8 est d'application. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.
Art. 16	Art. 16
§ 1er. A la fin des inspections, un rapport est dressé par le service d'inspection. Une copie de ce rapport est transmise à l'organisme d'évaluation de la conformité, au titulaire de certificats de cybersécurité européens ou à l'émetteur de déclarations de conformité de l'Union européenne inspecté.	§ 1er. A la fin des inspections, un rapport est dressé par le service d'inspection. Une copie de ce rapport est transmise à l'organisme d'évaluation de la conformité, au titulaire de certificats de cybersécurité européens ou à l'émetteur de déclarations de conformité de l'Union européenne inspecté.
§ 2. Les rapports dressés par le service d'inspection ne peuvent contenir, ni les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni les données à caractère personnel traitées par ces clients.	§ 2. Les rapports dressés par le service d'inspection ne peuvent contenir, ni les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni les données à caractère personnel traitées par ces clients.
§ 3. A leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, aux articles 58, paragraphe 7, c), et 60,	§ 3. A leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, aux articles 58, paragraphe 7, c), et 60,

paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications peut recevoir une copie du rapport visé au paragraphe 1er.	paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications peut recevoir une copie du rapport visé au paragraphe 1er.
Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de rapport prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que:	Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de rapport prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que:
1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;	1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;
2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;	2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;
3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;	3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;
4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.	4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.
§ 4. Dans le respect des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'autorité sectorielle et au service d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi précitée du 1er juillet 2011 et à l'article 7, § § 3 et 5, de la loi précitée du 7 avril 2019,	§ 4. Dans le respect **de l'article 17 de la loi du … relative à la résilience des entités critiques**, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'autorité sectorielle et au service d'inspection, visés respectivement **aux articles 3, 2° et 33 de la loi du … précitée,** compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12° à 14°, du Règlement sur la cybersécurité, lorsque ce rapport est lié à un contrôle effectué

compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12° à 14°, du Règlement sur la cybersécurité, lorsque ce rapport est lié à un contrôle effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi précitée du 1er juillet 2011 ou de la loi précitée du 7 avril 2019.	auprès d'une **entité critique, au sens de la loi précitée du ….**
Afin d'assurer le respect de l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en oeuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de l'arrêté royal précité du 2 décembre 2011, lorsque ce rapport est lié à un contrôle effectué auprès d'une infrastructure critique, au sens de cet arrêté royal.	Afin d'assurer le respect des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en oeuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du rapport prévu au paragraphe 1er à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, lorsque ce rapport est lié à un contrôle effectué auprès **d'une entité critique, au sens de la loi du … relative à la résilience des entités critiques.**
Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de rapport prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que:	Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de rapport prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que:
1° le transfert soit nécessaire à l'exécution de l'alinéa 2;	1° le transfert soit nécessaire à l'exécution de l'alinéa 2;
2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de l'arrêté royal du 2 décembre	2° l'autorité destinataire des données traite celles-ci dans le respect des **dispositions de la loi du … relative à la résilience des entités critiques,** de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien;	
3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;	3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;
4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.	4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.
Art. 17	Art. 17
§ 1er. Les membres assermentés du service d'inspection rédigent des procès-verbaux visés à l'article 20, § 1er.	§ 1er. Les membres assermentés du service d'inspection rédigent des procès-verbaux visés à l'article 20, § 1er.
§ 2. A leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil ainsi qu'aux articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications reçoit une copie d'un procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué par l'autorité visée à l'article 5, § 1er, ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2.	§ 2. A leur demande et pour autant que cela poursuive l'accomplissement des missions prévues à l'article VIII.30, § 2, du Code de droit économique, au chapitre II du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil ainsi qu'aux articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, l'autorité nationale d'accréditation ou l'Institut belge des services postaux et des télécommunications reçoit une copie d'un procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué par l'autorité visée à l'article 5, § 1er, ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2.
Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de procès-verbal prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que:	Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de procès-verbal prévue à l'alinéa 1er ne doit pas être formalisée par un protocole pour autant que:
1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;	1° le transfert soit nécessaire à l'exécution de l'alinéa 1er;

2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;	2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi, des articles 58, paragraphe 7, c), et 60, paragraphes 1er et 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques;
3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;	3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;
4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.	4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.
§ 3. Dans le respect de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet à l'autorité sectorielle et au service d'inspection compétents, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi précitée du 1er juillet 2011 et à l'article 7, § § 3 et 5, de la loi précitée du 7 avril 2019, en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, une copie complète du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi précitée du 1er juillet 2011 ou de la loi précitée du 7 avril 2019.	§ 3. Dans le respect **de article 18 de la loi du … relative à la résilience des entités critiques,** l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet à l'autorité sectorielle et au service d'inspection compétents, visés respectivement aux **articles 3, 2° et 33 de la loi du … précitée**, en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, une copie complète du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une **entité critique**, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la **loi précitée du …** ou de la loi précitée du 7 avril 2019.
Dans le respect de l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de	Dans le respect des sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée

base communes dans le domaine de la sûreté de l'aviation civile, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2, transmet une copie du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une infrastructure critique, au sens de l'article 2, 3°, de l'arrêté royal précité du 2 décembre 2011, à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de cet arrêté royal.	par le Roi en vertu de l'article 5, § 2, transmet une copie du procès-verbal ainsi que de toutes les informations complémentaires liées à un contrôle effectué auprès d'une **entité critique**, visée **à l'article 3, 3° de la loi du … relative à la résilience des entités critiques,** à l'inspection aéroportuaire, à l'inspection aéronautique ou à la Belgian Supervising Authority for Air Navigation Services, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de cet arrêté royal.
Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de procès-verbal prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que:	Par dérogation à l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la transmission de procès-verbal prévue au présent paragraphe ne doit pas être formalisée par un protocole pour autant que:
1° le transfert soit nécessaire à l'exécution de l'alinéa 2;	1° le transfert soit nécessaire à l'exécution de l'alinéa 2;
2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien;	2° l'autorité destinataire des données traite celles-ci dans le respect des dispositions **la loi du … relative à la résilience des entités critiques;**
3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;	3° le transfert concerne des données d'identification personnelle, comme un nom, un prénom, une adresse de courriel privée ou professionnelle, des données d'authentification ou des données de communications électroniques;
4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.	4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format numérique ou papier.
Art. 36	Art. 36
§ 1er. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:	§ 1er. Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:

1° la délivrance des certificats de cybersécurité européen et la gestion des réclamations y relatives par l'autorité visée à l'article 5, § 1er;	1° la délivrance des certificats de cybersécurité européen et la gestion des réclamations y relatives par l'autorité visée à l'article 5, § 1er;
2° le contrôle des titulaires de certificats de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne et des organismes d'évaluation de la conformité et, le cas échéant, l'imposition de sanctions conformément aux chapitres 5 et 6;	2° le contrôle des titulaires de certificats de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne et des organismes d'évaluation de la conformité et, le cas échéant, l'imposition de sanctions conformément aux chapitres 5 et 6;
3° la participation de l'autorité visée à l'article 5, § 1er, ou de toute autre autorité publique qui en fait la demande, au GECC;	3° la participation de l'autorité visée à l'article 5, § 1er, ou de toute autre autorité publique qui en fait la demande, au GECC;
4° la coopération avec les autorités sectorielles et les services d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, à l'article 7, § § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou aux articles 2, alinéa 1er, 1° et 9°, et 15, § § 1er à 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, dans le cadre de leurs pouvoirs visés à l'article 24, § 1er, de la loi précitée du 1er juillet 2011 ou aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, de la loi précitée du 7 avril 2019;	4° la coopération avec les autorités sectorielles et les services d'inspection, visés respectivement **aux articles 3, 2° et 33, de la loi du … relative à la résilience des entités critiques ou à l'article 15, § 2, de la loi du 24 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique** ou aux articles 2, alinéa 1er, 1° et 9, compétents en fonction du prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité, dans le cadre de leurs pouvoirs visés à l'article 24, § 1er, de la loi précitée du 1 juillet 2011 **ou aux articles 15, § 2, et 24 de la loi précitée du 24 avril 2024**;
5° la coopération avec les autorités publiques disposant de missions spécifiques en matière de cybersécurité, au sens de l'article 2, 1), du Règlement sur la cybersécurité, conformément à l'article 58, paragraphe 7, a), c) et h), du même règlement.	5° la coopération avec les autorités publiques disposant de missions spécifiques en matière de cybersécurité, au sens de l'article 2, 1), du Règlement sur la cybersécurité, conformément à l'article 58, paragraphe 7, a), c) et h), du même règlement.
§ 2. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 sont chacune responsables des traitements qu'elles effectuent pour la réalisation des finalités visées au paragraphe 1er.	§ 2. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 sont chacune responsables des traitements qu'elles effectuent pour la réalisation des finalités visées au paragraphe 1er.

§ 3. Les catégories de données à caractère personnel traitées par les responsables de traitement visés au paragraphe 2 sont les suivantes:	§ 3. Les catégories de données à caractère personnel traitées par les responsables de traitement visés au paragraphe 2 sont les suivantes:
1° pour la finalité visée au paragraphe 1er, 1°: les données d'identification de toute personne physique intervenant directement dans une demande de délivrance d'un certificat de cybersécurité européen ou dans une réclamation y relative par l'autorité visée à l'article 5, § 1er, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et l'adresse e-mail;	1° pour la finalité visée au paragraphe 1er, 1°: les données d'identification de toute personne physique intervenant directement dans une demande de délivrance d'un certificat de cybersécurité européen ou dans une réclamation y relative par l'autorité visée à l'article 5, § 1er, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et l'adresse e-mail;
2° pour la finalité visée au paragraphe 1er, 2°: toute donnée à caractère personnel nécessaire à l'exercice des missions de contrôle et de sanction visées aux chapitres 5 et 6;	2° pour la finalité visée au paragraphe 1er, 2°: toute donnée à caractère personnel nécessaire à l'exercice des missions de contrôle et de sanction visées aux chapitres 5 et 6;
3° pour la finalité visée au paragraphe 1er, 3°: les données d'identification des personnes physiques ayant vocation à participer au GECC, c'est-à-dire leur nom, leur prénom, leur adresse, leur numéro de téléphone et leur adresse e-mail;	3° pour la finalité visée au paragraphe 1er, 3°: les données d'identification des personnes physiques ayant vocation à participer au GECC, c'est-à-dire leur nom, leur prénom, leur adresse, leur numéro de téléphone et leur adresse e-mail;
4° pour la finalité visée au paragraphe 1er, 4°: les données d'identification, c'est-à-dire le nom, le prénom, l' adresse, le numéro de téléphone et l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients;	4° pour la finalité visée au paragraphe 1er, 4°: les données d'identification, c'est-à-dire le nom, le prénom, l' adresse, le numéro de téléphone et l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients;
5° pour la finalité visée au paragraphe 1er, 5°: les données d'identification, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et	5° pour la finalité visée au paragraphe 1er, 5°: les données d'identification, c'est-à-dire le nom, le prénom, l'adresse, le numéro de téléphone et

l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients.	l'adresse e-mail, ou les données de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 relative aux communications électroniques directement liées au prestataire ou fournisseur du produit TIC, service TIC ou processus TIC concerné, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité et collectées par le service d'inspection dans le cadre de ses missions de contrôle et de sanction visées aux chapitres 5 et 6, sans que ces données puissent porter sur les personnes physiques, clientes du titulaire de certificats de cybersécurité européens ou de l'émetteur de déclarations de conformité de l'Union européenne concerné, ou sur les données à caractère personnel traitées par ces clients.
Dans le cas mentionné à l'alinéa 1er, 2°, les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne et les données à caractère personnel traitées par ces clients, ne peuvent être traitées que si elles se révèlent nécessaires aux missions de contrôle visées au chapitre 5.	Dans le cas mentionné à l'alinéa 1er, 2°, les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne et les données à caractère personnel traitées par ces clients, ne peuvent être traitées que si elles se révèlent nécessaires aux missions de contrôle visées au chapitre 5.
Chaque fois que possible, les données visées à l'alinéa 2 sont pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ou les lois et règlements qui le complètent ou le précisent.	Chaque fois que possible, les données visées à l'alinéa 2 sont pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ou les lois et règlements qui le complètent ou le précisent.
§ 4. Sans préjudice du paragraphe 3, 2°, les échanges d'informations entre autorités publiques visés par la présente loi ne peuvent porter, ni sur les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni sur les données à caractère personnel traitées par ces clients.	§ 4. Sans préjudice du paragraphe 3, 2°, les échanges d'informations entre autorités publiques visés par la présente loi ne peuvent porter, ni sur les données à caractère personnel des clients des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne, ni sur les données à caractère personnel traitées par ces clients.

§ 5. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitements sont les suivantes:	§ 5. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet de traitements sont les suivantes:
1° toute personne physique intervenant pour les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne ou une autorité publique;	1° toute personne physique intervenant pour les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne ou une autorité publique;
2° toute personne physique participant à un contrôle ou à une audition dans le cadre des missions de contrôle prévues au chapitre 5;	2° toute personne physique participant à un contrôle ou à une audition dans le cadre des missions de contrôle prévues au chapitre 5;
3° toute personne physique introduisant une réclamation;	3° toute personne physique introduisant une réclamation;
4° toute personne physique participant au GECC;	4° toute personne physique participant au GECC;
5° toute personne physique dont les données à caractère personnel sont présentes au sein des produits TIC, services TIC ou processus TIC, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité.	5° toute personne physique dont les données à caractère personnel sont présentes au sein des produits TIC, services TIC ou processus TIC, au sens de l'article 2, 12) à 14), du Règlement sur la cybersécurité.

Loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications

Art. 14	Art. 14
§ 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, en ce qui concerne la lutte contre la diffusion des contenus à caractère terroriste en ligne au sens du règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, en ce qui concerne les services intermédiaires, en ce	§ 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, **relevant du secteur des infrastructures numériques, à l'exception des fournisseurs de services de confiance, au sens de la loi du … relative à la résilience des entités critiques**, en ce qui concerne la lutte contre la diffusion des contenus à caractère terroriste en ligne au sens du règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, en ce qui concerne les services intermédiaires, en ce qui concerne

qui concerne l'article XI.216/2, § 2, du Code de droit économique, et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes:	l'article XI.216/2, § 2, du Code de droit économique, et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes:
1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre, du ministre qui a l'Économie dans ses attributions et du membre du gouvernement qui a l'Agenda numérique dans ses attributions, dans la limite de leurs attributions respectives, ou de la Chambre des représentants;	1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre, du ministre qui a l'Économie dans ses attributions et du membre du gouvernement qui a l'Agenda numérique dans ses attributions, dans la limite de leurs attributions respectives, ou de la Chambre des représentants;
2° la prise de décisions administratives;	2° la prise de décisions administratives;
3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution:	3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution:
a) la loi du 13 juin 2005 relative aux communications électroniques;	a) la loi du 13 juin 2005 relative aux communications électroniques;
b) le Titre I^{er}, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;	b) le Titre I^{er}, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;
c) la loi du 26 janvier 2018 relative aux services postaux à l'exception des articles 3, § 2, alinéa 5, 5, § 1er, 5/2, 5/3, 5/4, 5/5 et 10/1;	c) la loi du 26 janvier 2018 relative aux services postaux à l'exception des articles 3, § 2, alinéa 5, 5, § 1er, 5/2, 5/3, 5/4, 5/5 et 10/1;
d) les articles 14, § 2, 2°, 15, 15/1 et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges;	d) les articles 14, § 2, 2°, 15, 15/1 et 21, §§ 5 à 7, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges;
e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;	e) les articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;
f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale;	f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale;
g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques;	**g) la loi du … relative à la résilience des entités critiques, en ce qui concerne le secteur de l'infrastructure numérique, à l'exception des fournisseurs de services de confiance**;

h) la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle et au service d'inspection sectoriel pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de la même loi;	h) la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne les tâches dévolues à l'autorité sectorielle et au service d'inspection sectoriel pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de la même loi;
i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques;	i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques;
j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques;	j) tout acte juridique contraignant en droit de l'Union européenne, qui attribue des missions à l'autorité réglementaire nationale dans le secteur des postes ou des communications électroniques;
k) toute décision contraignante adoptée par:	k) toute décision contraignante adoptée par:
i) l'Institut; ii) les ministres sur base de l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques; iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal;	i) l'Institut; ii) les ministres sur base de l'article 105, § 6, alinéa 1er, de la loi du 13 juin 2005 relative aux communications électroniques; iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal;
l) le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne, sans préjudice de tâches confiées à d'autres autorités compétentes en vertu de l'article 12, paragraphe 1er, a) et b), dudit règlement;	l) le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne, sans préjudice de tâches confiées à d'autres autorités compétentes en vertu de l'article 12, paragraphe 1er, a) et b), dudit règlement;
m) le règlement sur les services numériques.	m) le règlement sur les services numériques.
Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités	Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités

pratiques des inspections pour ce secteur, après avis de l'Institut.	pratiques des inspections pour ce secteur, après avis de l'Institut.
4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale,) la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;	4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, (ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale,) la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure;
4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques]12 ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ou en l'absence d'accord au sens de l'article XI.216/2, § 2, du Code de droit économique, la prise de décision administrative sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;	4° /1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de communications électroniques ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ou en l'absence d'accord au sens de l'article XI.216/2, § 2, du Code de droit économique,, la prise de décision administrative sur base de l'article 4 ou 4/1 de la loi du 17 janvier 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges;
5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.	5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications.
6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'État dans le secteur postal et dans le secteur des communications électroniques , sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques]6. L'Institut informe tant le	6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'État dans le secteur postal et dans le secteur des communications électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre

Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion;	en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion;
7° l'exercice des missions de contrôle et de sanctions qui lui sont confiées par l'arrêté royal visant à exécuter l'article 5, § 2, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité.	7° l'exercice des missions de contrôle et de sanctions qui lui sont confiées par l'arrêté royal visant à exécuter l'article 5, § 2, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité.
Pour l'application de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle au sens de l'article 8, 54°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1er, alinéa 2, de cette même loi pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi, et pour le secteur des services postaux et d'expédition.	Pour l'application de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle au sens de l'article 8, 54°, de cette même loi et service d'inspection sectoriel au sens de l'article 44, § 1er, alinéa 2, de cette même loi pour le secteur d'infrastructure numérique, à l'exception des prestataires de services de confiance au sens de l'article 8, 24°, de cette même loi, et pour le secteur des services postaux et d'expédition.
§ 1er/1. En ce qui concerne les compétences fédérales, l'Institut est une autorité compétente au sens de l'article 49 du règlement sur les services numériques.	§ 1er/1. En ce qui concerne les compétences fédérales, l'Institut est une autorité compétente au sens de l'article 49 du règlement sur les services numériques.
§ 2. Dans le cadre de ses compétences, l'Institut:	§ 2. Dans le cadre de ses compétences, l'Institut:
1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications	1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications

électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;	électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;
2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;	2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées;
3° coopère avec et communique de l'information à:	3° coopère avec et communique de l'information à:
a) la Commission européenne, l'ENISA, l'Office, l'ORECE et au Comité européen des services numériques;	a) la Commission européenne , l'ENISA, l'Office , l'ORECE et au Comité européen des services numériques;
b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;	b) les autorités de régulation étrangères en matière de services postaux et de télécommunications;
c) les autorités de régulation des autres secteurs économiques;	c) les autorités de régulation des autres secteurs économiques;
d) les services publics fédéraux en charge de la protection des consommateurs;	d) les services publics fédéraux en charge de la protection des consommateurs;
e) les autorités belges en charge de la concurrence;	e) les autorités belges en charge de la concurrence;
Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Économie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut;	Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Économie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut;
f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;	f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir;
g) les services publics qui ont une compétence en matière de sécurité publique, en ce compris la sécurité des réseaux et des systèmes d'information, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;	g) les services publics qui ont une compétence en matière de sécurité publique, en ce compris la sécurité des réseaux et des systèmes d'information, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays;
h) l'Autorité de protection des données;	h) l'Autorité de protection des données;

i) le Service public fédéral Économie, P.M.E., Classes moyennes et Énergie;	i) le Service public fédéral Économie, P.M.E., Classes moyennes et Énergie;
Après consultation de l'Institut et sur proposition conjointe du ministre qui a l'Economie dans ses attributions et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre le Service public fédéral visé à l'alinéa 1er et l'Institut;	Après consultation de l'Institut et sur proposition conjointe du ministre qui a l'Economie dans ses attributions et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre le Service public fédéral visé à l'alinéa 1er et l'Institut;
j) les ministres visés à l'article 105, § 1er, alinéa 3, 1°, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en œuvre de cet article;	j) les ministres visés à l'article 105, § 1er, alinéa 3, 1°, de la loi du 13 juin 2005 relative aux communications électroniques et leur cabinet, pour la mise en œuvre de cet article;
k) le Parquet fédéral et les autorités compétentes des autres États membres visées au règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne;	k) le Parquet fédéral et les autorités compétentes des autres États membres visées au règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère antiterroriste en ligne;
l) les inspecteurs sociaux de la Direction générale Contrôle des lois sociales du Service public fédéral Emploi, Travail et Concertation sociale, les inspecteurs sociaux de l'Inspection de l'Office national de Sécurité sociale, les inspecteurs sociaux de l'Inspection de l'Office national de l'Emploi et les inspecteurs sociaux de l'Institut national d'assurances sociales pour travailleurs indépendants;	l) les inspecteurs sociaux de la Direction générale Contrôle des lois sociales du Service public fédéral Emploi, Travail et Concertation sociale, les inspecteurs sociaux de l'Inspection de l'Office national de Sécurité sociale, les inspecteurs sociaux de l'Inspection de l'Office national de l'Emploi et les inspecteurs sociaux de l'Institut national d'assurances sociales pour travailleurs indépendants;
m) les coordinateurs pour les services numériques et les autres autorités compétentes au sens de l'article 49 du règlement sur les services numériques;	m) les coordinateurs pour les services numériques et les autres autorités compétentes au sens de l'article 49 du règlement sur les services numériques;
4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;	4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993;
5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.	5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques.

6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés:	6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés à l'article 6 de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 35 de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés:
- veiller à la qualité et à la pérennité du service universel; - veiller aux intérêts des utilisateurs des services postaux; - contribuer au développement d'un marché intérieur des services postaux; - promouvoir la concurrence dans le secteur postal;	- veiller à la qualité et à la pérennité du service universel; - veiller aux intérêts des utilisateurs des services postaux; - contribuer au développement d'un marché intérieur des services postaux; - promouvoir la concurrence dans le secteur postal;
7° peut, en sa qualité de service d'inspection, exiger à tout moment la communication du plan de sécurité de l'exploitant, en dérogation à l'article 25, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	**Abrogé.**
§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.	§ 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités.
§ 4. Sur proposition de l'Institut ou sur proposition conjointe du ministre qui a l'Économie dans ses attributions, du membre du gouvernement qui a l'Agenda numérique dans ses attributions et du ministre, après avis de l'Institut, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange	§ 4. Sur proposition de l'Institut ou sur proposition conjointe du ministre qui a l'Économie dans ses attributions, du membre du gouvernement qui a l'Agenda numérique dans ses attributions et du ministre, après avis de l'Institut, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange

d'informations entre l'Institut et les autres autorités sectorielles non encore visées au paragraphe 2, 3°, lorsque cela s'avère utile pour une application efficace du règlement sur les services numériques.	d'informations entre l'Institut et les autres autorités sectorielles non encore visées au paragraphe 2, 3°, lorsque cela s'avère utile pour une application efficace du règlement sur les services numériques.

Loi du 22 février 1998 portant le statut organique de la Banque nationale de Belgique

Art. 36/14	Art. 36/14
§ 1er. Par dérogation à l'article 35, la Banque peut également communiquer des informations confidentielles reçues dans l'exercice de ses missions visées à l'article 36/2, § 1er:	§ 1er. Par dérogation à l'article 35, la Banque peut également communiquer des informations confidentielles reçues dans l'exercice de ses missions visées à l'article 36/2, § 1er:
1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.	1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement.
Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des États membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.	Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des États membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier.

En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les États membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;	En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les États membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances;
2° dans les limites du droit de l'Union européenne, aux autorités compétentes de l'Union européenne et d'autres États membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3, y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement MSU;	2° dans les limites du droit de l'Union européenne, aux autorités compétentes de l'Union européenne et d'autres États membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3, y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement MSU;
2° /1 dans les limites du droit de l'Union européenne, aux autorités compétentes d'autres États membres de l'Espace économique européen qui exercent une ou plusieurs compétences de contrôle à l'égard des entités assujetties énumérées à l'article 2, paragraphe 1er, points 1) et 2) de la directive (UE) 2015/849, aux fins du respect de ladite directive et ce, pour l'exercice de la mission que cette directive leur confère;	2° /1 dans les limites du droit de l'Union européenne, aux autorités compétentes d'autres États membres de l'Espace économique européen qui exercent une ou plusieurs compétences de contrôle à l'égard des entités assujetties énumérées à l'article 2, paragraphe 1er, points 1) et 2) de la directive (UE) 2015/849, aux fins du respect de ladite directive et ce, pour l'exercice de la mission que cette directive leur confère;
3° dans le respect du droit de l'Union européenne, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 , en ce compris les autorités ayant des compétences de même nature que celles des autorités visées au 2° /1, et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations;	3° dans le respect du droit de l'Union européenne, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3, en ce compris les autorités ayant des compétences de même nature que celles des autorités visées au 2° /1, et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations;
4° à la FSMA;	4° à la FSMA;
5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution;	5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution;

6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;	6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;
7° dans les limites du droit de l'Union européenne, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent;	7° dans les limites du droit de l'Union européenne, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent;
8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;	8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;
9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires;	9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires;
10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque;	10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque;
11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'États membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque;	11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'États membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque;

12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence;	12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence;
13° …	13° ...
14° à l'Administration générale de la Trésorerie du Service public fédéral Finances lorsqu'une telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6°, de la loi du 18 septembre 2017) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;	14° à l'Administration générale de la Trésorerie du Service public fédéral Finances lorsqu'une telle communication est prévue par le droit de l'Union européenne ou par une disposition légale ou réglementaire en matière de sanctions financières (notamment les dispositions contraignantes relatives aux embargos financiers telles que définies à l'article 4, 6°, de la loi du 18 septembre 2017) ou lorsque l'Administration générale de la Trésorerie agit en qualité d'autorité de contrôle assurant le respect du règlement (CE) 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant;
15° dans les limites du droit de l'Union européenne, aux actuaires indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaires;	15° dans les limites du droit de l'Union européenne, aux actuaires indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaires;
16° à Fedris;	16° à Fedris;
17° dans les limites du droit de l'Union européenne, au Service Public Fédéral économie, en sa qualité d'autorité compétente pour assurer le contrôle des dispositions visées au livre VII, titres 1er à 3, titre 5, chapitre 1er, et titres 6 et 7 du Code de droit économique ainsi qu'aux agents commissionnés par le ministre qui dans le cadre de leur mission visée à l'article XV.2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV.89 dudit Code;	17° dans les limites du droit de l'Union européenne, au Service Public Fédéral économie, en sa qualité d'autorité compétente pour assurer le contrôle des dispositions visées au livre VII, titres 1er à 3, titre 5, chapitre 1er, et titres 6 et 7 du Code de droit économique ainsi qu'aux agents commissionnés par le ministre qui dans le cadre de leur mission visée à l'article XV.2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV.89 dudit Code;
18° aux autorités relevant du droit d'États membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement	18° aux autorités relevant du droit d'États membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement

(UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010;	(UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010;
19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne;	19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne;
20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application de l'article 19 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques le requiert;	20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application **de l'article 26 de la loi du … relative à la résilience des entités critiques l'exige;**
20° /1 dans les limites du droit de l'Union européenne, aux services de police et à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et au CSIRT national visé à l'article 8, 46°, de la même loi pour les besoins de l'exécution de l'article 53, § 2, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;	20° /1 dans les limites du droit de l'Union européenne, aux services de police et à l'autorité nationale de cybersécurité visée à l'article 8, 45°, de la loi NIS2 et au CSIRT national visé à l'article 8, 46°, de la même loi pour les besoins de l'exécution de l'article 53, § 2, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement;
20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;	20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er, de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, ou aux autorités désignées par le Roi en vertu de l'article 5, § 2, de la même loi;
21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au	21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au

contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43*bis*, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et leurs opérations;	contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43*bis*, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et leurs opérations;
22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des États membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution;	22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des États membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution;
22° /1 dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 du Règlement 2021/23, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12*ter*, § 1/1, avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des États membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou l'exécution d'une mesure de résolution;	22° /1 dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 du Règlement 2021/23, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12*ter*, § 1/1, avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des États membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou l'exécution d'une mesure de résolution;
23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment:	23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment:
a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit;	a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit;
b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au	b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au

statut et au contrôle des établissements de crédit; et	statut et au contrôle des établissements de crédit; et
c) le commissaire spécial et l'administrateur provisoire visés à l'article 236, § 1er, de la loi précitée du 25 avril 2014, à l'article 204, § 1er de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses, à l'article 517, § 1er, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 117, § 1er, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, l'article 215, § 1er, de la loi précitée, l'article 48, alinéa 1er, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, et l'article 36/30/1, § 2 de la présente loi;	c) le commissaire spécial et l'administrateur provisoire visés à l'article 236, § 1er, de la loi précitée du 25 avril 2014, à l'article 204, § 1er de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses, à l'article 517, § 1er, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 117, § 1er, de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, l'article 215, § 1er, de la loi précitée, l'article 48, alinéa 1er, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, et l'article 36/30/1, § 2 de la présente loi;
24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 15 de la loi NIS2 pour les besoins de l'exécution des dispositions de la loi NIS2 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;
25° au Service Public Fédéral Économie, P.M.E., Classes moyennes et Énergie dans l'exercice de sa mission visée à l'article 85, § 1er 5°, de la loi du 18 septembre 2017 à l'égard des entités visées à l'article 5, § 1er, 21°, de la même loi;	25° au Service Public Fédéral Économie, P.M.E., Classes moyennes et Énergie dans l'exercice de sa mission visée à l'article 85, § 1er 5°, de la loi du 18 septembre 2017 à l'égard des entités visées à l'article 5, § 1er, 21°, de la même loi;
26° dans les limites du droit de l'Union européenne, aux cellules de renseignement financier visées à l'article 4, 15° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;	26° dans les limites du droit de l'Union européenne, aux cellules de renseignement financier visées à l'article 4, 15° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;
27° en cas de détérioration de la situation financière d'un établissement financier visé à l'article 36/2, au Ministère public;	27° en cas de détérioration de la situation financière d'un établissement financier visé à l'article 36/2, au Ministère public;
28° dans les limites du droit de l'Union européenne, à la Commission européenne	28° dans les limites du droit de l'Union européenne, à la Commission européenne

lorsque ces informations sont nécessaires à l'exercice des compétences de cette dernière.	lorsque ces informations sont nécessaires à l'exercice des compétences de cette dernière.
§ 2. La Banque ne peut communiquer des informations confidentielles en vertu du paragraphe 1er qu'aux conditions suivantes:	§ 2. La Banque ne peut communiquer des informations confidentielles en vertu du paragraphe 1er qu'aux conditions suivantes:
1° les informations sont destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires, ce qui inclut la communication desdites informations à des tiers en application d'une obligation légale applicable à ces autorités ou organismes; dans les autres cas, la Banque peut autoriser, dans les limites du droit de l'Union européenne, les destinataires desdites informations à les divulguer à des tiers, moyennant l'accord préalable de la Banque et, le cas échéant, aux seules fins pour lesquelles la Banque a marqué son accord;	1° les informations sont destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires, ce qui inclut la communication desdites informations à des tiers en application d'une obligation légale applicable à ces autorités ou organismes; dans les autres cas, la Banque peut autoriser, dans les limites du droit de l'Union européenne, les destinataires desdites informations à les divulguer à des tiers, moyennant l'accord préalable de la Banque et, le cas échéant, aux seules fins pour lesquelles la Banque a marqué son accord;
2° les informations ainsi communiquées à des autorités ou organismes étrangers sont couvertes dans leur chef par une obligation de secret professionnel équivalente à celui prévu à l'article 35; et	2° les informations ainsi communiquées à des autorités ou organismes étrangers sont couvertes dans leur chef par une obligation de secret professionnel équivalente à celui prévu à l'article 35; et
3° lorsque les informations concernées proviennent d'une autorité d'un autre État membre de l'Espace économique européen, elles ne peuvent être divulguées aux autorités ou organismes suivants qu'avec l'accord explicite de l'autorité communicante et, le cas échéant, aux seules fins pour lesquelles cette dernière a marqué son accord:	3° lorsque les informations concernées proviennent d'une autorité d'un autre État membre de l'Espace économique européen, elles ne peuvent être divulguées aux autorités ou organismes suivants qu'avec l'accord explicite de l'autorité communicante et, le cas échéant, aux seules fins pour lesquelles cette dernière a marqué son accord:
a) les autorités ou organismes visés aux paragraphe 1er, 5°, 6°, 8° et 11°;	a) les autorités ou organismes visés aux paragraphe 1er, 5°, 6°, 8° et 11°;
b) les autorités ou organismes d'Etats tiers visés aux paragraphe 1er, 3°, 5°, 8°, 9°, 11°, 18° et 22°;	b) les autorités ou organismes d'Etats tiers visés aux paragraphe 1er, 3°, 5°, 8°, 9°, 11°, 18° et 22°;
c) les autorités ou organismes d'États tiers exerçant des missions équivalentes à celles de la FSMA.	c) les autorités ou organismes d'États tiers exerçant des missions équivalentes à celles de la FSMA.
§ 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes de droit belge visés au paragraphe 1er sont tenus au secret professionnel prévu à l'article 35 quant	§ 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes de droit belge visés au paragraphe 1er sont tenus au secret professionnel prévu à l'article 35 quant

aux informations confidentielles reçues de la Banque en application du paragraphe 1er.	aux informations confidentielles reçues de la Banque en application du paragraphe 1er.
Art. 36/49	Art. 36/49
La Banque est désignée comme autorité administrative dans le sens de l'article 22quinquies de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. La Banque est compétente pour les entités du secteur des finances qu'elle identifie comme infrastructures critiques en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	La Banque est désignée comme autorité administrative dans le sens de l'article 22quinquies de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. La Banque est compétente pour les entités du secteur des finances qu'elle identifie comme **entités critiques** en vertu de **la loi du … relative à la résilience des entités critiques.**
Loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations	
Art. 15/2*sexies*	Art. 15/2*sexies*
§ 1er. Le gestionnaire d'infrastructures non actives a le droit d'offrir aux entreprises fournissant ou autorisées à fournir des réseaux de communications électroniques l'accès à ses infrastructures non actives en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit.	§ 1er. Le gestionnaire d'infrastructures non actives a le droit d'offrir aux entreprises fournissant ou autorisées à fournir des réseaux de communications électroniques l'accès à ses infrastructures non actives en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit.
§ 2. En réponse à une demande écrite formulée par une entreprise fournissant ou autorisée à fournir des réseaux de communications publics, le gestionnaire d'infrastructures non actives fait droit à toute demande raisonnable d'accès à ses infrastructures non actives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.	§ 2. En réponse à une demande écrite formulée par une entreprise fournissant ou autorisée à fournir des réseaux de communications publics, le gestionnaire d'infrastructures non actives fait droit à toute demande raisonnable d'accès à ses infrastructures non actives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.
§ 3. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:	§ 3. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:
1° la capacité technique de l'infrastructure non active à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2;	1° la capacité technique de l'infrastructure non active à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2;

2° l'espace disponible pour accueillir des autres éléments du réseau de transport, du réseau fermé industriel ou de la conduite directe du gestionnaire d'infrastructures non actives, y compris les besoins futurs d'espace dudit gestionnaire, ou pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics qui a introduit la demande ou les éléments de réseaux d'autres entreprises, lesquels ont été démontrés de manière suffisante;	2° l'espace disponible pour accueillir des autres éléments du réseau de transport, du réseau fermé industriel ou de la conduite directe du gestionnaire d'infrastructures non actives, y compris les besoins futurs d'espace dudit gestionnaire, ou pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics qui a introduit la demande ou les éléments de réseaux d'autres entreprises, lesquels ont été démontrés de manière suffisante;
3° des considérations de sûreté et de santé publique;	3° des considérations de sûreté et de santé publique;
4° l'intégrité et la sécurité de l'infrastructure non active, en particulier de celle constituant une infrastructure critique nationale visée par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	4° l'intégrité et la sécurité de l'infrastructure non active, en particulier de celle constituant **une entité critique** visée **par la loi du … relative à la résilience des entités critiques**;
5° le risque d'interférence grave entre les services de communications électroniques en projet et les autres services fournis à l'aide des infrastructures non actives;	5° le risque d'interférence grave entre les services de communications électroniques en projet et les autres services fournis à l'aide des infrastructures non actives;
6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure non active, offerts par le gestionnaire d'infrastructures non actives et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.	6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure non active, offerts par le gestionnaire d'infrastructures non actives et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.
Le gestionnaire d'infrastructures non actives indique les raisons de son refus dans un délai de deux mois à compter de la date de réception de la demande d'accès complète.	Le gestionnaire d'infrastructures non actives indique les raisons de son refus dans un délai de deux mois à compter de la date de réception de la demande d'accès complète.
§ 4. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'organe de règlement	§ 4. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'organe de règlement

des litiges en matière d'infrastructures de réseaux.	des litiges en matière d'infrastructures de réseaux.
L'alinéa 1er est applicable sans préjudice de la possibilité pour toute partie, en cas de litige, de saisir le tribunal de première instance de Bruxelles, statuant comme en référé, conformément à la procédure fixée par l'article 15/2decies.	L'alinéa 1er est applicable sans préjudice de la possibilité pour toute partie, en cas de litige, de saisir le tribunal de première instance de Bruxelles, statuant comme en référé, conformément à la procédure fixée par l'article 15/2decies.
§ 5. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure non-active lorsque le gestionnaire d'infrastructures non actives n'est pas le propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics d'obtenir les permis et autorisations requis pour la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.	§ 5. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure non-active lorsque le gestionnaire d'infrastructures non actives n'est pas le propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics d'obtenir les permis et autorisations requis pour la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.

Loi du 29 avril 1999 relative à l'organisation du marché de l'électricité

Art. 14/1	Art. 14/1
§ 1er. Le gestionnaire d'infrastructures non actives a le droit d'offrir aux entreprises fournissant ou autorisées à fournir des réseaux de communications électroniques l'accès à ses infrastructures non actives en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit.	§ 1er. Le gestionnaire d'infrastructures non actives a le droit d'offrir aux entreprises fournissant ou autorisées à fournir des réseaux de communications électroniques l'accès à ses infrastructures non actives en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit.
§ 2. En réponse à une demande écrite formulée par une entreprise fournissant ou autorisée à fournir des réseaux de communications publics, le gestionnaire d'infrastructures non actives fait droit à toute demande raisonnable d'accès à ses infrastructures non actives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.	§ 2. En réponse à une demande écrite formulée par une entreprise fournissant ou autorisée à fournir des réseaux de communications publics, le gestionnaire d'infrastructures non actives fait droit à toute demande raisonnable d'accès à ses infrastructures non actives selon des modalités et des conditions équitables et raisonnables, y compris au niveau du prix, en vue du déploiement d'éléments de réseaux de communications électroniques à haut débit. Cette demande écrite indique de manière détaillée les éléments du projet pour lequel l'accès est demandé, y compris un échéancier précis.

§ 3. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:	§ 3. Tout refus d'accès est fondé sur des critères objectifs, transparents et proportionnés, tels que:
1° la capacité technique de l'infrastructure non active à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2;	1° la capacité technique de l'infrastructure non active à laquelle l'accès a été demandé d'accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2;
2° l'espace disponible pour des autres éléments du réseau de transport, du réseau fermé industriel, du raccordement ou de la ligne directe du gestionnaire d'infrastructures non actives, y compris les besoins futurs d'espace dudit gestionnaire, ou pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics, qui a introduit la demande, ou les éléments de réseaux d'autres entreprises, lesquels ont été démontrés de manière suffisante;	2° l'espace disponible pour des autres éléments du réseau de transport, du réseau fermé industriel, du raccordement ou de la ligne directe du gestionnaire d'infrastructures non actives, y compris les besoins futurs d'espace dudit gestionnaire, ou pour accueillir les éléments de réseaux de communications électroniques à haut débit visés au paragraphe 2, y compris les besoins futurs d'espace de l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics, qui a introduit la demande, ou les éléments de réseaux d'autres entreprises, lesquels ont été démontrés de manière suffisante;
3° des considérations de sûreté et de santé publique;	3° des considérations de sûreté et de santé publique;
4° l'intégrité et la sécurité de l'infrastructure non active, en particulier de celle constituant une infrastructure critique nationale visée par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	4° l'intégrité et la sécurité de l'infrastructure non active, en particulier de celle constituant **une entité critique** visée **par la loi du … relative à la résilience des entités critiques;**
5° le risque d'interférence grave entre les services de communications électroniques en projet et les autres services fournis à l'aide des infrastructures non actives;	5° le risque d'interférence grave entre les services de communications électroniques en projet et les autres services fournis à l'aide des infrastructures non actives;
6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure non active, offerts par le gestionnaire d'infrastructures non actives et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.	6° la disponibilité d'autres moyens viables de fourniture en gros d'accès physique à l'infrastructure non active, offerts par le gestionnaire d'infrastructures non actives et adaptés à la fourniture de réseaux de communications électroniques à haut débit, pour autant que l'accès soit offert selon des modalités et des conditions équitables et raisonnables.
Le gestionnaire d'infrastructures non actives indique les raisons de son refus dans un délai de	Le gestionnaire d'infrastructures non actives indique les raisons de son refus dans un délai de

deux mois à compter de la date de réception de la demande d'accès complète.	deux mois à compter de la date de réception de la demande d'accès complète.
§ 4. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'organe de règlement des litiges en matière d'infrastructures de réseaux.	§ 4. Si l'accès est refusé ou si aucun accord n'a été trouvé sur les modalités et conditions spécifiques, y compris le prix, dans un délai de deux mois à compter de la date de réception de la demande d'accès, chaque partie est habilitée à porter l'affaire devant l'organe de règlement des litiges en matière d'infrastructures de réseaux.
L'alinéa 1er est applicable sans préjudice de la possibilité pour toute partie, en cas de litige, de saisir le tribunal de première instance de Bruxelles, statuant comme en référé, conformément à la procédure fixée par l'article 14/5.	L'alinéa 1er est applicable sans préjudice de la possibilité pour toute partie, en cas de litige, de saisir le tribunal de première instance de Bruxelles, statuant comme en référé, conformément à la procédure fixée par l'article 14/5.
§ 5. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure non active lorsque le gestionnaire d'infrastructures non-actives n'est pas le propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics d'obtenir les permis et autorisations requis pour la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.	§ 5. Le présent article s'entend sans préjudice du droit de propriété du propriétaire de l'infrastructure non active lorsque le gestionnaire d'infrastructures non-actives n'est pas le propriétaire ainsi que du droit de propriété de tout autre tiers, tels que les propriétaires fonciers et les propriétaires privés. Le présent article s'entend également sans préjudice de l'obligation pour l'entreprise fournissant ou autorisée à fournir des réseaux de communications publics d'obtenir les permis et autorisations requis pour la pose des éléments constitutifs de son réseau de communications électroniques à haut débit.

Code pénal

Art. 546/2	Art. 546/2
§ 1. L'infraction visée à l'article 546/1 est punie d'un emprisonnement de huit jours à un an et d'une amende de vingt-six euros à mille euros ou d'une de ces peines seulement:	§ 1. L'infraction visée à l'article 546/1 est punie d'un emprisonnement de huit jours à un an et d'une amende de vingt-six euros à mille euros ou d'une de ces peines seulement:
1° lorsque l'activité concernée constitue une activité habituelle;	1° lorsque l'activité concernée constitue une activité habituelle;
2° si elle a été commise pendant la nuit;	2° si elle a été commise pendant la nuit;
3° si elle a été commise par deux personnes ou plus;	3° si elle a été commise par deux personnes ou plus;

4° si elle a été commise avec une intention frauduleuse ou à dessein de nuire;	4° si elle a été commise avec une intention frauduleuse ou à dessein de nuire;
5° si elle a été commise à l'aide de violences ou de menaces;	5° si elle a été commise à l'aide de violences ou de menaces;
6° si la personne est entrée ou a fait intrusion dans une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	**6° si une entité critique, au sens de la loi du … sur la résilience des entités critiques, a fait l'objet d'une entrée ou d'une intrusion.**
§ 2. La tentative de commettre l'infraction visée au paragraphe 1er du présent article est punie d'un emprisonnement de huit jours à six mois et d'une amende de vingt-six euros à cinq cents euros ou d'une de ces peines seulement.	§ 2. La tentative de commettre l'infraction visée au paragraphe 1er du présent article est punie d'un emprisonnement de huit jours à six mois et d'une amende de vingt-six euros à cinq cents euros ou d'une de ces peines seulement.
Art. 550*ter*	Art. 550*ter*
§ 1er. Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.	§ 1er. Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.
Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.	Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de six mois à cinq ans.
La même peine sera appliquée lorsque l'infraction visée à l'alinéa 1er est commise contre un système informatique d'une infrastructure critique comme visée dans l'article 3, 4°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	**La même peine est appliquée lorsque l'infraction visée à l'alinéa 1er est commise à l'encontre d'un système d'information d'une entité critique telle que visée à l'article 3, 3°, de la loi du … relative à la résilience des entités critiques.**
§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à septante-cinq mille [euros] ou d'une de ces peines seulement.	§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six [euros] à septante-cinq mille [euros] ou d'une de ces peines seulement.

§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement.	§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement.
§ 4. Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.	§ 4. Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.
§ 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*.	§ 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210*bis*, 259*bis*, 314*bis*, 504*quater* ou 550*bis*.
§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.	§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.

Loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 15*bis*	Art. 15*bis*
Conformément à l'article 24 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et à ses arrêtés d'exécution, l'Agence est chargée de contrôler l'application des dispositions de ladite loi aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité, qui servent au transport de l'électricité et qui ont été désignés comme infrastructure critique en vertu de la loi du 1er juillet 2011 susmentionnée.	Conformément à **l'article 33 de la loi du … relative à la résilience des entités critiques** et à ses arrêtés d'exécution, l'Agence est chargée de contrôler l'application des dispositions de ladite loi aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité, qui servent au transport de l'électricité et qui ont été **désignés comme entité critique en vertu de la loi du … relative à la résilience des entités critiques.**
Les modalités du contrôle sont réglées par le Roi.	Les modalités du contrôle sont réglées par le Roi.

Loi du 10 juillet 2006 relative à l'analyse de la menace

Art. 6	Art. 6
§ 1er. Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements portant sur les menaces visées à l'article 3, les personnes et les groupements, auteurs ou cibles éventuels de menace, et les événements, dont ils disposent dans le cadre de leurs missions légales de prévention et de suivi du terrorisme et de l'extrémisme au sens de l'article 8, 1°, b) et c), de la loi organique des services de renseignement et de sécurité et qui s'avèrent pertinents en vue d'atteindre les finalités des évaluations communes visées à l'article 8, alinéa 1er, 1° et 2°.	§ 1er. Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements portant sur les menaces visées à l'article 3, les personnes et les groupements, auteurs ou cibles éventuels de menace, et les événements, dont ils disposent dans le cadre de leurs missions légales de prévention et de suivi du terrorisme et de l'extrémisme au sens de l'article 8, 1°, b) et c), de la loi organique des services de renseignement et de sécurité et qui s'avèrent pertinents en vue d'atteindre les finalités des évaluations communes visées à l'article 8, alinéa 1er, 1° et 2°.
Lorsqu'il y a des raisons de croire que l'intégrité de personnes physiques se trouve en danger concret et imminent, liées à des menaces extrémistes ou terroristes, le directeur peut exiger des services d'appui la communication immédiate des données à caractère personnel et des renseignements visés à l'alinéa 1er. Le directeur motive sa demande sur la nécessité de transmettre immédiatement les données à caractère personnel et les renseignements.	Lorsqu'il y a des raisons de croire que l'intégrité de personnes physiques se trouve en danger concret et imminent, liées à des menaces extrémistes ou terroristes, le directeur peut exiger des services d'appui la communication immédiate des données à caractère personnel et des renseignements visés à l'alinéa 1er. Le directeur motive sa demande sur la nécessité de transmettre immédiatement les données à caractère personnel et les renseignements.
	Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'article 9, § 2, de la loi du … relative à la résilience des entités critiques.

§ 2. Le Roi détermine, par arrêté délibéré en Conseil des ministres, et après avis du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité, les modalités d'accès, de communication et d'effacement des données à caractère personnel et des renseignements visés au paragraphe 1er.	§ 2. Le Roi détermine, par arrêté délibéré en Conseil des ministres, et après avis du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité, les modalités d'accès, de communication et d'effacement des données à caractère personnel et des renseignements visés au paragraphe 1er.

Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Art. 3	Art. 3
§ 1er. Dans les limites de l'article 4 et sans préjudice de l'article 6, la présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II et qui constituent:	§ 1er. Dans les limites de l'article 4 et sans préjudice de l'article 6, la présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II et qui constituent:
1° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou	1° une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE; ou
2° une entreprise qui dépasse les plafonds prévus au paragraphe 1er du même article de cette annexe.	2° une entreprise qui dépasse les plafonds prévus au paragraphe 1er du même article de cette annexe.
L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.	L'article 3, § 4, de l'annexe de la recommandation n° 2003/361/CE ne s'applique pas aux fins de la présente loi.
§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation n° 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit.	§ 2. Dans le cadre de l'application de l'article 6, paragraphe 2, de l'annexe de la recommandation n° 2003/361/CE, l'autorité nationale de cybersécurité tient compte du degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées, en particulier en ce qui concerne les réseaux et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit.
Sur base de l'alinéa 1er, l'autorité nationale de cybersécurité considère qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d'indépendance de ladite entité, celle-ci n'aurait pas été considérée comme constituant une entreprise moyenne ou	Sur base de l'alinéa 1er, l'autorité nationale de cybersécurité considère qu'une telle entité ne constitue pas une entreprise moyenne en vertu de l'article 2 de l'annexe de la recommandation n° 2003/361/CE, ou ne dépasse pas les plafonds applicables à une entreprise moyenne prévus au paragraphe 1 dudit article, si, après prise en compte du degré d'indépendance de ladite entité, celle-ci n'aurait pas été considérée comme constituant une entreprise moyenne ou

dépassant lesdits plafonds si seules ses propres données avaient été prises en compte.	dépassant lesdits plafonds si seules ses propres données avaient été prises en compte.
Le Roi peut déterminer les critères sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.	Le Roi peut déterminer les critères sur base desquels le degré d'indépendance dont jouit une entité à l'égard de ses partenaires et de ses entreprises liées est évalué.
§ 3. Sans préjudice de l'article 6, la présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans un des cas suivants:	§ 3. Sans préjudice de l'article 6, la présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans un des cas suivants:
1° les services sont fournis par:	1° les services sont fournis par:
a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public; b) des prestataires de services de confiance; c) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;	a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public; b) des prestataires de services de confiance; c) des registres de noms de domaine de premier niveau et des fournisseurs de services de systèmes de noms de domaine;
2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;	2° l'entité est identifiée comme une entité essentielle ou importante conformément au chapitre 4 du présent titre;
3° l'entité est une entité de l'administration publique:	3° l'entité est une entité de l'administration publique:
a) qui dépend de l'État fédéral; b) qui dépend des entités fédérées, identifiée conformément à l'article 11, § 2; c) qui est une zone de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale au sens de l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale.	a) qui dépend de l'État fédéral; b) qui dépend des entités fédérées, identifiée conformément à l'article 11, § 2; c) qui est une zone de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale au sens de l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale.
§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	§ 4. Sans préjudice de l'article 6, quelle que soit leur taille, la présente loi s'applique aux entités identifiées comme **entités critiques au sens de la loi du … relative à la résilience des entités critiques.**

§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.	§ 5. Quelle que soit leur taille, la présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine.
§ 6. Après consultation des éventuelles autorités sectorielles concernées et de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs et/ou sous-secteurs à l'annexe I ou II ou élargir les secteurs et/ou sous-secteurs existants.	§ 6. Après consultation des éventuelles autorités sectorielles concernées et de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs et/ou sous-secteurs à l'annexe I ou II ou élargir les secteurs et/ou sous-secteurs existants.
Art. 8	Art. 8
Pour l'application de la présente loi, il faut entendre par:	Pour l'application de la présente loi, il faut entendre par:
1° "réseau et système d'information":	1° "réseau et système d'information":
a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;	a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;
b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou	b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; ou
c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;	c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;
2° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;	2° "sécurité des réseaux et des systèmes d'information": la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;

3° “cybersécurité”: la cybersécurité au sens de l’article 2, 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l’ENISA (Agence de l’Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l’information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), ci-après le “règlement sur la cybersécurité”;	3° “cybersécurité”: la cybersécurité au sens de l’article 2, 1), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l’ENISA (Agence de l’Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l’information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), ci-après le “règlement sur la cybersécurité”;
4° “stratégie nationale en matière de cybersécurité”: le cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser en Belgique;	4° “stratégie nationale en matière de cybersécurité”: le cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser en Belgique;
5° “incident”: un événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles;	5° “incident”: un événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles;
6° “incident évité”: un événement qui aurait pu compromettre la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s’est pas produite;	6° “incident évité”: un événement qui aurait pu compromettre la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s’est pas produite;
7° “incident de cybersécurité majeur”: un incident qui provoque des perturbations dépassant les capacités de réaction du seul Etat membre de l’Union européenne concerné ou qui a un impact significatif sur au moins deux États membres de l’Union européenne;	7° “incident de cybersécurité majeur”: un incident qui provoque des perturbations dépassant les capacités de réaction du seul Etat membre de l’Union européenne concerné ou qui a un impact significatif sur au moins deux États membres de l’Union européenne;
8° “traitement des incidents”: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;	8° “traitement des incidents”: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;
9° “risque”: le potentiel de perte ou de perturbation à la suite d’un incident, à exprimer comme la combinaison de l’ampleur d’une telle perte ou d’une telle perturbation et de la probabilité qu’un tel incident se produise;	9° “risque”: le potentiel de perte ou de perturbation à la suite d’un incident, à exprimer comme la combinaison de l’ampleur d’une telle perte ou d’une telle perturbation et de la probabilité qu’un tel incident se produise;

10° “cybermenace”: une cybermenace visée à l’article 2, point 8), du règlement sur la cybersécurité;	10° “cybermenace”: une cybermenace visée à l’article 2, point 8), du règlement sur la cybersécurité;
11° “cybermenace importante”: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d’avoir un impact grave sur les réseaux et les systèmes d’information d’une entité ou les utilisateurs des services de l’entité, en causant un dommage matériel, corporel ou moral considérable;	11° “cybermenace importante”: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d’avoir un impact grave sur les réseaux et les systèmes d’information d’une entité ou les utilisateurs des services de l’entité, en causant un dommage matériel, corporel ou moral considérable;
12° “produit TIC”: un produit TIC au sens de l’article 2, 12), du règlement sur la cybersécurité;	12° “produit TIC”: un produit TIC au sens de l’article 2, 12), du règlement sur la cybersécurité;
13° “service TIC”: un service TIC au sens de l’article 2, 13), du règlement sur la cybersécurité;	13° “service TIC”: un service TIC au sens de l’article 2, 13), du règlement sur la cybersécurité;
14° “processus TIC”: un processus TIC au sens de l’article 2, 14), du règlement sur la cybersécurité;	14° “processus TIC”: un processus TIC au sens de l’article 2, 14), du règlement sur la cybersécurité;
15° “vulnérabilité”: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;	15° “vulnérabilité”: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;
16° “norme”: une norme au sens de l’article 2, 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ci-après le “règlement (UE) n°1025/2012”;	16° “norme”: une norme au sens de l’article 2, 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ci-après le “règlement (UE) n°1025/2012”;
17° “point d’échange internet”: une structure de réseau qui permet l’interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l’échange de trafic internet, qui n’assure l’interconnexion que pour des systèmes autonomes et qui n’exige pas que le trafic internet passant entre une paire quelconque de	17° “point d’échange internet”: une structure de réseau qui permet l’interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l’échange de trafic internet, qui n’assure l’interconnexion que pour des systèmes autonomes et qui n’exige pas que le trafic internet passant entre une paire quelconque de

systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;	systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;
18° "système de nom de domaine" ou "DNS": un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;	18° "système de nom de domaine" ou "DNS": un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;
19° "fournisseur de services DNS": une entité qui fournit:	19° "fournisseur de services DNS": une entité qui fournit:
a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou	a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou
b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;	b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;
20° "registre de noms de domaine de premier niveau": une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;	20° "registre de noms de domaine de premier niveau": une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;
21° "entité fournissant des services d'enregistrement de noms de domaine": un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;	21° "entité fournissant des services d'enregistrement de noms de domaine": un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

22° “service numérique”: un service au sens de l’article 1er, paragraphe 1er, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d’information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l’information;	22° “service numérique”: un service au sens de l’article 1er, paragraphe 1er, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d’information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l’information;
23° “service de confiance”: un service de confiance au sens de l’article 3, 16, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le “règlement eIDAS”;	23° “service de confiance”: un service de confiance au sens de l’article 3, 16, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le “règlement eIDAS”;
24° “prestataire de services de confiance”: un prestataire de services de confiance au sens de l’article 3, 19, du règlement eIDAS;	24° “prestataire de services de confiance”: un prestataire de services de confiance au sens de l’article 3, 19, du règlement eIDAS;
25° “service de confiance qualifié”: un service de confiance qualifié au sens de l’article 3, 17, du règlement eIDAS;	25° “service de confiance qualifié”: un service de confiance qualifié au sens de l’article 3, 17, du règlement eIDAS;
26° “prestataire de services de confiance qualifiés”: un prestataire de services de confiance qualifié au sens de l’article 3, 20, du règlement eIDAS;	26° “prestataire de services de confiance qualifiés”: un prestataire de services de confiance qualifié au sens de l’article 3, 20, du règlement eIDAS;
27° “place de marché en ligne”: une place de marché en ligne au sens de l’article I.8, 41°, du Code de droit économique;	27° “place de marché en ligne”: une place de marché en ligne au sens de l’article I.8, 41°, du Code de droit économique;
28° “moteur de recherche en ligne”: un moteur de recherche en ligne au sens de l’article 2, 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l’équité et la transparence pour les entreprises utilisatrices de services d’intermédiation en ligne;	28° “moteur de recherche en ligne”: un moteur de recherche en ligne au sens de l’article 2, 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l’équité et la transparence pour les entreprises utilisatrices de services d’intermédiation en ligne;
29° “service d’informatique en nuage”: un service numérique qui permet l’administration à la demande et l’accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;	29° “service d’informatique en nuage”: un service numérique qui permet l’administration à la demande et l’accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

30° “service de centre de données”: un service qui englobe les structures, ou groupes de structures, dédiées à l’hébergement, l’interconnexion et l’exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l’ensemble des installations et infrastructures de distribution d’électricité et de contrôle environnemental;	30° “service de centre de données”: un service qui englobe les structures, ou groupes de structures, dédiées à l’hébergement, l’interconnexion et l’exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l’ensemble des installations et infrastructures de distribution d’électricité et de contrôle environnemental;
31° “réseau de diffusion de contenu”: un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l’accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d’internet pour le compte de fournisseurs de contenu et de services;	31° “réseau de diffusion de contenu”: un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l’accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d’internet pour le compte de fournisseurs de contenu et de services;
32° “plateforme de services de réseaux sociaux”: une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;	32° “plateforme de services de réseaux sociaux”: une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;
33° “représentant”: une personne physique ou morale établie dans l’Union européenne qui est expressément désignée pour agir pour le compte d’un fournisseur de services DNS, d’un registre de noms de domaine de premier niveau, d’une entité fournissant des services d’enregistrement de noms de domaine, d’un fournisseur d’informatique en nuage, d’un fournisseur de services de centre de données, d’un fournisseur de réseau de diffusion de contenu, d’un fournisseur de services gérés, d’un fournisseur de services de sécurité gérés ou d’un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l’Union européenne, qui peut être contactée par l’autorité nationale de cybersécurité à la place de l’entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi;	33° “représentant”: une personne physique ou morale établie dans l’Union européenne qui est expressément désignée pour agir pour le compte d’un fournisseur de services DNS, d’un registre de noms de domaine de premier niveau, d’une entité fournissant des services d’enregistrement de noms de domaine, d’un fournisseur d’informatique en nuage, d’un fournisseur de services de centre de données, d’un fournisseur de réseau de diffusion de contenu, d’un fournisseur de services gérés, d’un fournisseur de services de sécurité gérés ou d’un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l’Union européenne, qui peut être contactée par l’autorité nationale de cybersécurité à la place de l’entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi;
34° “entité de l’administration publique”: une autorité administrative visée à l’article 14, § 1er,	34° “entité de l’administration publique”: une autorité administrative visée à l’article 14, § 1er,

alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants:	alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants:
a) elle n'a pas de caractère industriel ou commercial; b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi; c) elle n'est pas une personne morale de droit privé.	a) elle n'a pas de caractère industriel ou commercial; b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi; c) elle n'est pas une personne morale de droit privé.
35° "réseau de communications électroniques public": un réseau public de communications électroniques au sens de l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques;	35° "réseau de communications électroniques public": un réseau public de communications électroniques au sens de l'article 2, 10°, de la loi du 13 juin 2005 relative aux communications électroniques;
36° "service de communications électroniques": un service de communications électroniques au sens de l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques;	36° "service de communications électroniques": un service de communications électroniques au sens de l'article 2, 5°, de la loi du 13 juin 2005 relative aux communications électroniques;
37° "entité": une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;	37° "entité": une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;
38° "fournisseur de services gérés": une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;	38° "fournisseur de services gérés": une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;
39° "fournisseur de services de sécurité gérés": un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;	39° "fournisseur de services de sécurité gérés": un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;
40° "organisme de recherche": une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement;	40° "organisme de recherche": une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement;

41° “recommandation n° 2003/361/CE”: la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;	41° “recommandation n° 2003/361/CE”: la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises;
42° “loi du 13 juin 2005”: la loi du 13 juin 2005 relative aux communications électroniques;	42° “loi du 13 juin 2005”: la loi du 13 juin 2005 relative aux communications électroniques;
43° “loi du 1er juillet 2011”: la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	43° **loi du …: la loi du […] relative à la résilience des entités critiques;**
44° “arrêté royal du 18 avril 1988”: l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;	44° “arrêté royal du 18 avril 1988”: l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;
45° “autorité nationale de cybersécurité”: l’autorité visée à l’article 16;	45° “autorité nationale de cybersécurité”: l’autorité visée à l’article 16;
46° “CSIRT national”: le centre national de réponse aux incidents de sécurité informatique;	46° “CSIRT national”: le centre national de réponse aux incidents de sécurité informatique;
47° “ENISA”: l’Agence de l’Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;	47° “ENISA”: l’Agence de l’Union européenne pour la cybersécurité instituée par le règlement sur la cybersécurité;
48° “NCCN”: le Centre institué par l’arrêté royal du 18 avril 1988;	48° “NCCN”: le Centre institué par l’arrêté royal du 18 avril 1988;
49° “règlement (UE) 2016/679”: le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);	49° “règlement (UE) 2016/679”: le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);
50° “autorité de protection des données”: autorité de contrôle au sens de l’article 4, 21°, du règlement (UE) 2016/679;	50° “autorité de protection des données”: autorité de contrôle au sens de l’article 4, 21°, du règlement (UE) 2016/679;
51° “organisme national d’accréditation”: l’organisme visé à l’article 2, point 11, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l’accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après le “règlement (CE) n° 765/2008”;	51° “organisme national d’accréditation”: l’organisme visé à l’article 2, point 11, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l’accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, ci-après le “règlement (CE) n° 765/2008”;

52° “politique de sécurité des systèmes et réseaux d’information (“P.S.I.”)”: la politique consignée dans un document visé à l’article 30, reprenant les mesures de sécurité des réseaux et des systèmes d’information, à adopter par une entité essentielle ou importante;	52° “politique de sécurité des systèmes et réseaux d’information (“P.S.I.”)”: la politique consignée dans un document visé à l’article 30, reprenant les mesures de sécurité des réseaux et des systèmes d’information, à adopter par une entité essentielle ou importante;
53° “organisme d’évaluation de la conformité”: l’organisme visé à l’article 2, point 13, du règlement (CE) n° 765/2008;	53° “organisme d’évaluation de la conformité”: l’organisme visé à l’article 2, point 13, du règlement (CE) n° 765/2008;
54° “autorité sectorielle”: l’autorité visée à l’article 15, § 2;	54° “autorité sectorielle”: l’autorité visée à l’article 15, § 2;
55° “réseau des CSIRT”: le réseau des CSIRT nationaux institué par l’article 15 de la directive NIS2;	55° “réseau des CSIRT”: le réseau des CSIRT nationaux institué par l’article 15 de la directive NIS2;
56° “groupe de coopération”: le groupe de coopération établi par l’article 14 de la directive NIS2;	56° “groupe de coopération”: le groupe de coopération établi par l’article 14 de la directive NIS2;
57° “incident significatif”: tout incident ayant un impact significatif sur la fourniture de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II de la loi et qui:	57° “incident significatif”: tout incident ayant un impact significatif sur la fourniture de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II de la loi et qui:
1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II ou des pertes financières pour l’entité concernée; ou	1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l’un des services fournis dans les secteurs ou sous-secteurs repris à l’annexe I et II ou des pertes financières pour l’entité concernée; ou
2° a affecté ou est susceptible d’affecter d’autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.	2° a affecté ou est susceptible d’affecter d’autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.
58° “crise cyber”: tout incident de cybersécurité qui, par sa nature ou ses conséquences:	58° “crise cyber”: tout incident de cybersécurité qui, par sa nature ou ses conséquences:
1° menace les intérêts vitaux du pays ou les besoins essentiels de la population; 2° requiert des décisions urgentes; 3° demande une action coordonnée de plusieurs départements et organisations.	1° menace les intérêts vitaux du pays ou les besoins essentiels de la population; 2° requiert des décisions urgentes; 3° demande une action coordonnée de plusieurs départements et organisations.
59° “Institut”: l’Institut belge des services postaux et des télécommunications tel que visé à l’article 13 de la loi du 17 janvier 2003 relative	59° “Institut”: l’Institut belge des services postaux et des télécommunications tel que visé à l’article 13 de la loi du 17 janvier 2003 relative

au statut du régulateur des secteurs des postes et des télécommunications belges.	au statut du régulateur des secteurs des postes et des télécommunications belges.
Art. 15	Art. 15
§ 1er. Le Roi désigne l'autorité nationale de cybersécurité.	§ 1er. Le Roi désigne l'autorité nationale de cybersécurité.
§ 2. Après avis de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner une autorité sectorielle et, le cas échéant, un service d'inspection sectoriel chargé, pour un secteur ou sous-secteur spécifique, de la supervision de la mise en œuvre des mesures sectorielles ou sous-sectorielles supplémentaires de gestion des risques en matière de cybersécurité visées à l'article 33.	§ 2. Après avis de l'autorité nationale de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, désigner une autorité sectorielle et, le cas échéant, un service d'inspection sectoriel chargé, pour un secteur ou sous-secteur spécifique, de la supervision de la mise en œuvre des mesures sectorielles ou sous-sectorielles supplémentaires de gestion des risques en matière de cybersécurité visées à l'article 33.
Dans le cadre de la désignation visée à l'alinéa 1er, le Roi tient compte de l'identité des autorités sectorielles et services d'inspection sectoriels désignées dans le cadre de la loi du 1er juillet 2011.	Dans le cadre de la désignation visée à l'alinéa 1er, le Roi tient compte de l'identité des autorités sectorielles et services d'inspection sectoriels désignées dans le cadre de la **loi du ….**
Le Roi peut, par arrêté délibéré en Conseil des ministres, créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92ter de la loi spéciale du 8 août 1980 de réformes institutionnelles.	Le Roi peut, par arrêté délibéré en Conseil des ministres, créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92ter de la loi spéciale du 8 août 1980 de réformes institutionnelles.
Par dérogation à l'alinéa 1er, la présente loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régis par la loi.	Par dérogation à l'alinéa 1er, la présente loi désigne elle-même les autorités sectorielles et les services d'inspection créés et régis par la loi.
Art. 25	Art. 25
§ 1er. Les autorités visées au chapitre 1er du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.	§ 1er. Les autorités visées au chapitre 1er du présent titre coopèrent les unes avec les autres afin de respecter les obligations énoncées dans la présente loi.
§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1er coopèrent également, au niveau national, avec le NCCN, les services administratifs de l'État, les autorités administratives, en ce compris les autorités nationales en vertu des règlements (CE) n° 300/2008 et n° 2018/1139, les organes de	§ 2. En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1er coopèrent également, au niveau national, avec le NCCN, les services administratifs de l'État, les autorités administratives, en ce compris les autorités nationales en vertu des règlements (CE) n° 300/2008 et n° 2018/1139, les organes de

contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque Nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi du 1er juillet 2011, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de protection des données.	contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque Nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en **vertu de la loi du …,** les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de protection des données.
§ 3. Les entités essentielles et importantes et les autorités visées au chapitre 1er du présent titre collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.	§ 3. Les entités essentielles et importantes et les autorités visées au chapitre 1er du présent titre collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.
§ 4. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes dans le cadre de la loi du 1er juillet 2011 coopèrent et échangent régulièrement des informations sur le recensement des infrastructures critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les exploitants d'infrastructures recensées en tant qu'infrastructures critiques en vertu de la loi du 1er juillet 2011 et sur les mesures prises pour faire face à ces risques, menaces et incidents.	§ 4. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes dans le cadre **de la loi du …** coopèrent et échangent régulièrement des informations sur le recensement des infrastructures critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent **les entités critiques au sens de la loi du …** et sur les mesures prises pour faire face à ces risques, menaces et incidents.
§ 5. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 13 juin 2005, échangent	§ 5. Les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 13 juin 2005, échangent

régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.	régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.
§ 6. L'autorité nationale de cybersécurité crée une plateforme de coordination et d'évaluation afin que les autorités visées à l'article 15 et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la présente loi.	§ 6. L'autorité nationale de cybersécurité crée une plateforme de coordination et d'évaluation afin que les autorités visées à l'article 15 et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la présente loi.
Art. 28	Art. 28
§ 1er. Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les cinq ans, sur la base d'indicateurs de performance, après avis du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN et, le cas échéant, des autorités de protection des données.	§ 1er. Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les cinq ans, sur la base d'indicateurs de performance, après avis du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN et, le cas échéant, des autorités de protection des données.
Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et règlementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.	Cette stratégie définit les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et règlementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.
§ 2. La stratégie nationale en matière de cybersécurité comprend, entre autres:	§ 2. La stratégie nationale en matière de cybersécurité comprend, entre autres:
1° les objectifs et les priorités de la stratégie nationale en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;	1° les objectifs et les priorités de la stratégie nationale en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;
2° un cadre de gouvernance visant à atteindre les objectifs et les priorités visés au 1°, y compris les tâches et les responsabilités des autorités publiques et des autres acteurs concernés ainsi que les politiques visées au paragraphe 3;	2° un cadre de gouvernance visant à atteindre les objectifs et les priorités visés au 1°, y compris les tâches et les responsabilités des autorités publiques et des autres acteurs concernés ainsi que les politiques visées au paragraphe 3;
3° un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes en Belgique, et sur lequel reposent la coopération et la coordination, en Belgique, entre les autorités visées au chapitre 1er du présent titre ainsi que la coopération et la coordination entre ces autorités et les autorités compétentes en vertu d'instruments juridiques sectoriels de l'Union européenne;	3° un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes en Belgique, et sur lequel reposent la coopération et la coordination, en Belgique, entre les autorités visées au chapitre 1er du présent titre ainsi que la coopération et la coordination entre ces autorités et les autorités compétentes en vertu d'instruments juridiques sectoriels de l'Union européenne;

4° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;	4° un mécanisme visant à identifier les actifs pertinents et une évaluation des risques en Belgique;
5° un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;	5° un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;
6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;	6° une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;
7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu de la loi du 1er juillet 2011 aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;	7° un cadre politique visant une coordination renforcée entre les autorités visées au chapitre 1er du présent titre et les autorités compétentes en vertu de **la loi du …** aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;
8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;	8° un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité;
9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;	9° un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de cybersécurité;
10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.	10° un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de cybersécurité.
§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont adoptées et portent sur les éléments suivants:	§ 3. Des politiques, parties intégrantes de la stratégie nationale en matière de cybersécurité, sont adoptées et portent sur les éléments suivants:
1° la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services;	1° la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services;
2° l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes;	2° l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes;

3° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;	3° la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités conformément à l'article 22;
4° le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;	4° le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;
5° la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;	5° la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;
6° la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et de développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;	6° la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et de développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;
7° le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;	7° le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;
8° la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités;	8° la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités;
9° le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;	9° le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;
10° la promotion d'une cyberprotection active.	10° la promotion d'une cyberprotection active.

Art. 37	Art. 37
§ 1er. Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard injustifié les autres États membres touchés et l'ENISA de l'incident significatif. Sont alors partagées des informations du type de celles reçues conformément à l'article 35. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.	§ 1er. Lorsque c'est approprié, et notamment si l'incident significatif concerne deux États membres ou plus, le CSIRT national informe sans retard injustifié les autres États membres touchés et l'ENISA de l'incident significatif. Sont alors partagées des informations du type de celles reçues conformément à l'article 35. Ce faisant, le CSIRT national doit, dans le respect du droit de l'Union européenne ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.
§ 2. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou lorsque la divulgation de l'incident significatif est par ailleurs dans l'intérêt public, le CSIRT national peut, après avoir consulté l'entité concernée, le NCCN, l'éventuelle autorité sectorielle concernée et le ministre concerné, informer le public de l'incident significatif ou exiger de l'entité qu'elle le fasse.	§ 2. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident significatif ou pour faire face à un incident significatif en cours, ou lorsque la divulgation de l'incident significatif est par ailleurs dans l'intérêt public, le CSIRT national peut, après avoir consulté l'entité concernée, le NCCN, l'éventuelle autorité sectorielle concernée et le ministre concerné, informer le public de l'incident significatif ou exiger de l'entité qu'elle le fasse.
§ 3. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1er, alinéa 1er, aux points de contact uniques des autres États membres touchés.	§ 3. À la demande de l'éventuelle autorité sectorielle concernée, l'autorité nationale de cybersécurité transmet les notifications reçues en vertu de l'article 34, § 1er, alinéa 1er, aux points de contact uniques des autres États membres touchés.
§ 4. L'autorité nationale de cybersécurité soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er.	§ 4. L'autorité nationale de cybersécurité soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément à l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er.
§ 5. Le CSIRT national fournit aux autorités compétentes en vertu de la loi du 1er juillet 2011 des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er, par les exploitants d'infrastructures identifiées comme infrastructures critiques en vertu de la loi du 1er juillet 2011.	§ 5. Le CSIRT national fournit aux autorités compétentes en vertu de **la loi du …** des informations sur les incidents significatifs, les incidents, les cybermenaces et les incidents évités notifiés conformément l'article 34, § 1er, alinéa 1er, et à l'article 38, § 1er, par **les entités critiques au sens de la loi du ….**

Art. 40	Art. 40
§ 1er. L'évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°, est effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité selon les conditions fixées par le Roi.	§ 1er. L'évaluation périodique de la conformité visée à l'article 39, alinéa 1er, 1°, est effectuée par un organisme d'évaluation de la conformité agréé par l'autorité nationale de cybersécurité selon les conditions fixées par le Roi.
Pour le contrôle des entités identifiées comme exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011 et des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui évaluent la conformité disposent d'une habilitation de sécurité.	Pour le contrôle **des entités critiques au sens de la loi du …** et des entités de l'administration publique, l'organisme d'évaluation de la conformité ainsi que les personnes physiques qui évaluent la conformité disposent d'une habilitation de sécurité.
§ 2. Le service d'inspection de l'autorité nationale de cybersécurité peut à tout moment vérifier le respect des conditions d'agrément visées au paragraphe 1er par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.	§ 2. Le service d'inspection de l'autorité nationale de cybersécurité peut à tout moment vérifier le respect des conditions d'agrément visées au paragraphe 1er par les organismes d'évaluation de la conformité, conformément aux dispositions du présent chapitre.
Art. 45	Art. 45
§ 1er. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent les autorités compétentes en vertu de la loi du 1er juillet 2011 lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'un exploitant d'une infrastructure identifiée comme critique en vertu de la loi du 1er juillet 2011 respecte la présente loi. Le cas échéant, les autorités compétentes en vertu de la loi du 1er juillet 2011 peuvent demander au service d'inspection de l'autorité nationale de cybersécurité et à l'éventuelle autorité sectorielle ou à l'éventuel service d'inspection sectoriel compétents d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'un exploitant d'une infrastructure qui est identifiée comme infrastructure critique en vertu de la loi du 1er juillet 2011.	§ 1er. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent les autorités compétentes en vertu de **la loi du …** lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir **qu'une entité critique au sens de la loi du …** respecte la présente loi. Le cas échéant, les autorités compétentes en vertu **de la loi du …** peuvent demander au service d'inspection de l'autorité nationale de cybersécurité et à l'éventuelle autorité sectorielle ou à l'éventuel service d'inspection sectoriel compétents d'exercer leurs pouvoirs de supervision et d'exécution à l'égard **d'une entité critique au sens de la loi du ….**
§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents coopèrent avec les autorités compétentes pertinentes en	§ 2. Le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents coopèrent avec les autorités compétentes pertinentes en

vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, dudit règlement lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle ou importante qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.	vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. En particulier, le service d'inspection de l'autorité nationale de cybersécurité et l'éventuelle autorité sectorielle ou l'éventuel service d'inspection sectoriel compétents informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, dudit règlement lorsqu'ils exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle ou importante qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.
Art. 67	Art. 67
Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:	Les finalités pour lesquelles des traitements de données à caractère personnel sont effectués, sont les suivantes:
1° l'amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;	1° l'amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;
2° l'exécution des tâches de l'autorité nationale de cybersécurité, notamment l'identification des entités, l'information et la sensibilisation des utilisateurs des systèmes d'information et de communication, l'octroi de subventions, la coopération internationale entre l'autorité nationale de cybersécurité, des autorités compétentes des autres États membres, des forums internationaux de cybersécurité, l'ENISA et la Commission européenne;	2° l'exécution des tâches de l'autorité nationale de cybersécurité, notamment l'identification des entités, l'information et la sensibilisation des utilisateurs des systèmes d'information et de communication, l'octroi de subventions, la coopération internationale entre l'autorité nationale de cybersécurité, des autorités compétentes des autres États membres, des forums internationaux de cybersécurité, l'ENISA et la Commission européenne;
3° la gestion des crises cyber et incidents de cybersécurité;	3° la gestion des crises cyber et incidents de cybersécurité;
4° l'exécution des tâches du CSIRT national visées aux articles suivants:	4° l'exécution des tâches du CSIRT national visées aux articles suivants:
a) 19, § 1er;	a) 19, § 1er;

b) 21, § 2, alinéa 2, 1° à 3°; c) 22, §§ 2 à 6; d) 37, §§ 1er à 3 et § 5;	b) 21, § 2, alinéa 2, 1° à 3°; c) 22, §§ 2 à 6; d) 37, §§ 1er à 3 et § 5;
5° la coopération, notamment l'échange d'informations entre l'autorité nationale de cybersécurité, les éventuelles autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de la loi du 1er juillet 2011, ainsi que les autorités visées à l'article 25, § 2, dans le cadre de l'exécution de la présente loi et la loi du 1er juillet 2011;	5° la coopération, notamment l'échange d'informations entre l'autorité nationale de cybersécurité, les éventuelles autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de **la loi du …,** ainsi que les autorités visées à l'article 25, § 2, dans le cadre de l'exécution de la présente loi **et la loi du …;**
6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1er;	6° la coopération entre les entités essentielles et importantes et les autorités visées au titre 2, chapitre 1er;
7° le partage d'informations entre les autorités visées à l'article 25, § 5;	7° le partage d'informations entre les autorités visées à l'article 25, § 5;
8° la continuité des services prestés par les entités importantes ou essentielles;	8° la continuité des services prestés par les entités importantes ou essentielles;
9° la notification d'incidents et d'incidents évités;	9° la notification d'incidents et d'incidents évités;
10° le contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives.	10° le contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives.
Art. 68	Art. 68
Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes:	Les catégories de données à caractère personnel traitées par les responsables de traitement sont les suivantes:
1° pour la finalité visée à l'article 67, 1°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les missions d'amélioration de la cybersécurité, de renforcement des politiques de prévention et de sécurité, de prévention des incidents de sécurité et de défense contre les cybermenaces visées à l'article 67, 1°;	1° pour la finalité visée à l'article 67, 1°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les missions d'amélioration de la cybersécurité, de renforcement des politiques de prévention et de sécurité, de prévention des incidents de sécurité et de défense contre les cybermenaces visées à l'article 67, 1°;
2° pour la finalité visée à l'article 67, 2°: les données d'identification, de connexion, de localisation et de communications électroniques	2° pour la finalité visée à l'article 67, 2°: les données d'identification, de connexion, de localisation et de communications électroniques

au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exécution des tâches de l'autorité nationale de cybersécurité;	au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exécution des tâches de l'autorité nationale de cybersécurité;
3° pour la finalité visée à l'article 67, 3°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les crises cyber et incidents de cybersécurité;	3° pour la finalité visée à l'article 67, 3°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par les crises cyber et incidents de cybersécurité;
4° pour la finalité visée à l'article 67, 4°: les données d'identification, de connexion, de localisation, de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 et des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005, des personnes concernées par l'exécution des tâches du CSIRT;	4° pour la finalité visée à l'article 67, 4°: les données d'identification, de connexion, de localisation, de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005 et des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005, des personnes concernées par l'exécution des tâches du CSIRT;
5° pour la finalité visée à l'article 67, 5°: les données d'identification des personnes concernées par la coopération dans le cadre de la loi du 1er juillet 2011;	5° pour la finalité visée à l'article 67, 5°: les données d'identification des personnes concernées par la coopération dans le cadre de **la loi du …;**
6° pour la finalité visée à l'article 67, 6°: les données d'identification des personnes concernées par la coopération;	6° pour la finalité visée à l'article 67, 6°: les données d'identification des personnes concernées par la coopération;
7° pour la finalité visée à l'article 67, 7°: les données d'identification des personnes concernées par le partage d'informations;	7° pour la finalité visée à l'article 67, 7°: les données d'identification des personnes concernées par le partage d'informations;
8° pour la finalité visée à l'article 67, 8°: les données d'identification des personnes concernées par l'assurance d'une continuité des services;	8° pour la finalité visée à l'article 67, 8°: les données d'identification des personnes concernées par l'assurance d'une continuité des services;
9° pour la finalité visée à l'article 67, 9°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exercice de notification;	9° pour la finalité visée à l'article 67, 9°: les données d'identification, de connexion, de localisation et de communications électroniques au sens de l'article 2, 91°, de la loi du 13 juin 2005, des personnes concernées par l'exercice de notification;
10° pour la finalité visée à l'article 67, 10°: les données à caractère personnel nécessaires et pertinentes à l'exercice des missions de contrôle, de supervision et de sanction, des personnes concernées par ces contrôles, cette supervision ou ces sanctions.	10° pour la finalité visée à l'article 67, 10°: les données à caractère personnel nécessaires et pertinentes à l'exercice des missions de contrôle, de supervision et de sanction, des personnes concernées par ces contrôles, cette supervision ou ces sanctions.

Centrale drukkerij - Imprimerie centrale