DOC 55 **2693/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

24 mai 2022

PROJET DE LOI

relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

24 mei 2022

WETSONTWERP

inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

INHOUD Blz.

07022

Le gouvernement a déposé ce projet de loi le 24 mai 2022.	*De regering heeft dit wetsontwerp op 24 mei 2022 ingediend.*
Le "bon à tirer" a été reçu à la Chambre le 25 mai 2022.	*De "goedkeuring tot drukken" werd op 25 mei 2022 door de Kamer ontvangen.*

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

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

RÉSUMÉ

Ce projet de loi vise à mettre en œuvre le 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, ci-après : le "Règlement sur la cybersécurité" (ou en anglais Cybersecurity Act – "CSA"). Ce règlement exige l'adoption de dispositions en droit national afin de le mettre en œuvre, notamment pour les inspections, réclamations, recours, sanctions, collaboration entre autorités.

Ce projet de loi est relatif à la certification de cybersécurité des technologies de l'information et des communications et porte désignation d'une autorité nationale de certification de cybersécurité ("ANCC").

Le Règlement sur la cybersécurité crée un cadre pour la délivrance et la reconnaissance mutuelle de certificats européens liés à la cybersécurité. En établissant un système européen harmonisé de certifications en matière de cybersécurité, le Règlement sur la cybersécurité vise à accroître la transparence de l'assurance en matière de cybersécurité des produits, services et processus des technologies de l'information et des communications (ci-après "TIC") et, partant, de renforcer la confiance dans le marché intérieur numérique ainsi que sa compétitivité.

Le recours aux certifications prévues par le Règlement sur la cybersécurité demeure volontaire. Toutefois, chaque État membre peut décider éventuellement de rendre obligatoires certaines de ces certifications, ce qui est encadré également par le présent projet. L'utilisation de certificats de cybersécurité pourra aussi faciliter les contrôles des autorités sectorielles ou de surveillance de marché.

Les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivreront, en principe, les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel". L'ANCC sera elle chargée de délivrer les certifications au niveau d'assurance élevé dans notre pays.

L'ANCC devra également s'assurer que toutes les règles liées à ce règlement seront correctement appliquées dans notre pays. Cette autorité sera également le représentant national au sein du Groupe européen de certification de cybersécurité (GECC).

SAMENVATTING

Dit wetsontwerp geeft uitvoering aan 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, hierna de "Cyberbeveiligingsverordening" (of in het Engels Cybersecurity Act – "CSA"). Om deze verordening uit te voeren, moeten bepalingen worden ingevoerd in het nationaal recht, met name voor inspecties, klachten, beroepen, sancties en de samenwerking tussen overheden.

Dit wetsontwerp heeft betrekking op de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en voorziet in de aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit ("NCCA").

De Cyberbeveiligingsverordening biedt een kader voor de afgifte en wederzijdse erkenning van Europese cyberbeveiligingscertificaten. Ze voert een geharmoniseerd Europees cyberbeveiligingscertificeringssysteem in om de transparantie van de cyberbeveiligingszekerheid van producten, diensten en processen op het gebied van informatie- en communicatietechnologie (hierna "ICT"), en daarmee het vertrouwen in en het concurrentievermogen van de digitale interne markt, te vergroten.

Het gebruik van de certificeringen waarin de Cyberbeveiligingsverordening voorziet, blijft vrijwillig. Elke lidstaat kan echter beslissen om sommige van deze certificeringen verplicht te maken, wat ook in dit ontwerp wordt geregeld. Het gebruik van cyberbeveiligingscertificaten kan ook controles door sectorale overheden of markttoezichtautoriteiten vergemakkelijken.

Conformiteitsbeoordelingsinstanties die door de nationale accreditatie-instantie zijn geaccrediteerd, zullen in principe Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" afgeven. De NCCA zal verantwoordelijk zijn voor de afgifte van certificeringen voor zekerheidsniveau "hoog" in ons land.

De NCCA zal er ook op moeten toezien dat alle regels in verband met deze verordening correct worden toegepast in ons land. Deze autoriteit zal ook de nationale vertegenwoordiger zijn in de Europese Groep voor cyberbeveiligingscertificering (EGC).

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

Ce projet de loi vise à mettre en œuvre le 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, désigné ci-après le "Règlement sur la cybersécurité".

Cette mise en œuvre exige, en effet, l'adoption de certaines dispositions légales en droit interne pour fixer notamment: les pouvoirs des services d'inspection, les règles de sanctions, les procédures de réclamations et de recours, les habilitations légales pour effectuer certaines délégations, les règles générales d'indépendance, etc.

COMMENTAIRE DES ARTICLES

CHAPITRE 1ER

Définitions et dispositions générales

Section 1re

Objet et champ d'application

Sous-section 1re

Objet

Cette section précise le fondement légal et l'objet du projet de loi.

L'autorité fédérale est compétente en cette matière car elle relève de la protection des consommateurs ainsi que de la sécurité publique, deux compétences fédérales.

En effet, le Règlement sur la cybersécurité a, selon ses considérants 7 et 10, pour but de renforcer la confiance des consommateurs auprès des fournisseurs de services numériques et de faire en sorte que les consommateurs disposent d'informations précises sur le niveau d'assurance auquel la sécurité de leur produits TIC, services TIC et processus TIC a été certifiée. Pour rappel, la Cour constitutionnelle a jugé, dans son arrêt

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Dit wetsontwerp geeft uitvoering aan 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, hierna de "Cyberbeveiligingsverordening" genoemd.

Deze uitvoering vereist immers de invoering van een aantal wettelijke bepalingen in het nationaal recht om met name de bevoegdheden van de inspectiediensten, de sanctieregels, de klachten- en beroepsprocedures, de wettelijke machtigingen voor bepaalde delegaties, de algemene onafhankelijkheidsregels, enz. vast te stellen.

TOELICHTING BIJ DE ARTIKELEN

HOOFDSTUK 1

Definities en algemene bepalingen

Afdeling 1

Onderwerp en toepassingsgebied

Onderafdeling 1

Onderwerp

Deze afdeling verduidelijkt de wettelijke grondslag en het onderwerp van het wetsontwerp.

De federale overheid is bevoegd voor deze materie aangezien consumentenbescherming en openbare veiligheid twee federale bevoegdheden zijn.

Volgens overwegingen 7 en 10 heeft de Cyberbeveiligingsverordening immers tot doel het vertrouwen van consumenten in digitaledienstverleners te versterken en ervoor te zorgen dat consumenten over nauwkeurige informatie beschikken met betrekking tot het zekerheidsniveau waarop hun ICT-producten, -diensten en -processen zijn gecertificeerd. Ter herinnering, in zijn arrest nr. 101/2013 van 9 juli 2013 oordeelde het

n° 101/2013 du 9 juillet 2013 que "*L'autorité fédérale est habilitée à fixer les règles générales en matière de protection des consommateurs*" et ce, conformément à l'article 6, § 1er, VI, alinéa 4, 2°, de la loi spéciale du 8 août 1980 de réformes institutionnelles.

De plus, le Règlement sur la cybersécurité a également pour objectif d'atténuer les risques liés à une numérisation et une connectivité accrue, rendant, selon le considérant 3, "*l'ensemble de la société plus vulnérable aux cybermenaces et* [exacerbant] *les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants*". À cette fin, le Règlement entend "*prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin que les réseaux et systèmes d'information, les réseaux de communication, les produits, services et appareils numériques utilisés par les citoyens, les organisations et les entreprises – depuis les petites et moyennes entreprises (PME), telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission, jusqu'aux opérateurs d'infrastructures critiques – soient mieux protégés contre les cybermenaces*", toujours selon le même considérant. Il en ressort clairement que le Règlement sur la cybersécurité porte sur la sécurité publique. Comme l'a rappelé la section de législation du Conseil d'État à plusieurs reprises, notamment dans ses avis n° 35 678, 43 644/4 et 63 972/4, "*les règles relatives à la sécurité publique demeurent en principe de la compétence de l'autorité fédérale*".

Sous-section 2

Champ d'application

Art. 3

Cet article précise que les certifications de cybersécurité prévues par la présente loi peuvent porter sur plusieurs types d'objet, définis à l'article 2, 12), 13), et 14), du Règlement sur la cybersécurité: un produit TIC (un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information), un service TIC (un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information) ou encore un processus TIC (un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance).

En effet, les organisations, les fabricants ou les fournisseurs impliqués dans la conception et le développement de produits TIC, services TIC ou processus TIC devraient être encouragés à mettre en œuvre, aux stades les plus précoces de la conception et du développement, des

Grondwettelijk Hof het volgende: "*De federale overheid is ertoe gemachtigd de algemene regels inzake consumentenbescherming vast te stellen*" en dit overeenkomstig artikel 6, § 1, VI, vierde lid, 2°, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

Voorts heeft de Cyberbeveiligingsverordening tot doel de risico's te beperken die verbonden zijn aan de toenemende digitalisering en connectiviteit. Volgens overweging 3 leiden die risico's ertoe dat "*de maatschappij als geheel kwetsbaarder wordt voor cyberdreigingen en […] de gevaren waaraan individuen, waaronder kwetsbare personen zoals kinderen, zijn blootgesteld worden vergerd*". Volgens dezelfde overweging wil de verordening daartoe "*alle noodzakelijke maatregelen [nemen] om de cyberbeveiliging in de Unie te versterken, zodat netwerk- en informatiesystemen, communicatienetwerken, digitale producten, diensten en toestellen die worden gebruikt door burgers, organisaties en bedrijven – van kleine en middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie tot exploitanten van cruciale infrastructuurvoorzieningen – beter beschermd worden tegen cyberdreigingen*". Hieruit blijkt duidelijk dat de Cyberbeveiligingsverordening betrekking heeft op openbare veiligheid. De afdeling wetgeving van de Raad van State heeft er herhaaldelijk op gewezen, met name in zijn adviezen nrs 35 678, 43 644/4 en 63 972/4, dat "*de federale overheid in principe bevoegd blijft voor de regels inzake openbare veiligheid*" (vrije vertaling).

Onderafdeling 2

Toepassingsgebied

Art. 3

Volgens dit artikel kunnen de in deze wet bedoelde cyberbeveiligingscertificeringen betrekking hebben op verschillende soorten zaken, bepaald in artikel 2, 12), 13) en 14), van de Cyberbeveiligingsverordening: een ICT-product (een element of groep elementen van een netwerk- of informatiesysteem), een ICT-dienst (een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen) of een ICT-proces (een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden).

Organisaties, fabrikanten en aanbieders die betrokken zijn bij het ontwerp en de ontwikkeling van ICT-producten, -diensten en -processen moeten er immers toe worden aangespoord om al in de eerste fase van ontwerp en ontwikkeling maatregelen te treffen om ervoor te zorgen

mesures permettant de protéger au mieux la sécurité de ces produits, services et processus, de manière que la survenance de cyberattaques soit présumée et que leur incidence soit anticipée et minimisée. La sécurité devrait être prise en charge tout au long du cycle de vie du produit TIC, service TIC ou processus TIC par les processus de conception et de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante.

À l'exception des articles 21 et 22, les chapitres 5 et 6 de la loi ne sont pas applicables aux certifications européennes rendues obligatoires en vertu du droit de l'Union ou du droit national. Les articles 21 et 22 visent, en effet, le retrait, la suspension ou la limitation d'un certificat, d'une autorisation ou d'une délégation. Il s'agit d'une prérogative de l'autorité nationale de certification de cybersécurité, que l'on soit dans une certification volontaire ou obligatoire.

Le paragraphe 2, alinéa 2, prévoit que l'autorité nationale de certification de cybersécurité applique les dispositions relatives à la mise en demeure et au recours, lorsqu'elle compte faire usage des prérogatives prévues aux articles 21 et 22 dans le cadre de certification obligatoire.

Les chapitres 5 et 6 (à l'exception des articles 21 et 22) ne sont pas applicables aux certifications obligatoires car ces dernières poursuivent, le cas échéant, un but plus spécifique justifiant des règles de contrôle et de sanctions différentes. En effet, dans le cadre de la certification de cybersécurité volontaire, le régime légal a pour but de renforcer, de manière générale, la confiance des consommateurs et la sécurité publique en proposant des certifications de cybersécurité auxquelles les personnes peuvent choisir de se soumettre. Lorsqu'une certification de cybersécurité est rendue obligatoire en vertu du droit de l'Union ou du droit national, le régime légal poursuit un but plus spécifique: imposer auprès de certaines entités l'obtention du certificat de cybersécurité concerné. À partir du moment où l'obtention d'un certificat de cybersécurité est considéré comme nécessaire et devient une obligation légale, des contrôles et des sanctions plus strictes peuvent se justifier.

Le Roi peut néanmoins décider, à l'initiative de cette autorité publique et si cela s'avère nécessaire, de lui accorder les mêmes pouvoirs de contrôle et de sanctions que ceux attribués à l'autorité nationale de certification de cybersécurité, assortis des mêmes possibilités de recours pour les certifications volontaires et visés aux chapitres 5 et 6 de la loi.

dat het beveiligingsniveau van deze producten, diensten en processen zo hoog mogelijk is, zodat cyberaanvallen zijn ingecalculeerd en de gevolgen daarvan zijn ingeschat en tot een minimum beperkt. Beveiliging moet tijdens de gehele levensduur van het ICT-product, de ICT-dienst of het ICT-proces worden gewaarborgd door middel van ontwerp- en ontwikkelingsprocessen die constant evolueren om het risico op schade door kwaadwillig gebruik te verminderen.

Met uitzondering van de artikelen 21 en 22 zijn de hoofdstukken 5 en 6 van de wet niet van toepassing op Europese certificeringen die verplicht zijn op grond van de Europese of nationale wetgeving. Artikel 21 en 22 hebben immers betrekking op de intrekking, opschorting of beperking van een certificaat, een toelating of een delegatie. Dit is een bevoegdheid van de nationale cyberbeveiligingscertificeringsautoriteit, ongeacht of het om een vrijwillige of verplichte certificering gaat.

Paragraaf 2, tweede lid, bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit de bepalingen betreffende de ingebrekestelling en het beroep toepast, indien ze van plan is gebruik te maken van de bevoegdheden bedoeld in artikel 21 en 22 in het kader van de verplichte certificering.

De hoofdstukken 5 en 6 (met uitzondering van artikel 21 en 22) zijn niet van toepassing op verplichte certificeringen omdat die laatste in voorkomend geval een specifieker doel nastreven, dat andere toezicht- en sanctieregels rechtvaardigt. In het kader van de vrijwillige cyberbeveiligingscertificering heeft de wettelijke regeling immers tot doel om, in het algemeen, het consumentenvertrouwen te vergroten en de openbare veiligheid te verhogen door cyberbeveiligingscertificeringen aan te bieden waaraan personen zich vrijwillig kunnen onderwerpen. Indien een cyberbeveiligingscertificering krachtens het recht van de Unie of het nationale recht wordt opgelegd, streeft de wettelijke regeling een specifieker doel na: bij bepaalde entiteiten het verkrijgen van het betrokken cyberbeveiligingscertificaat opleggen. Vanaf het ogenblik dat het verkrijgen van een cyberbeveiligingscertificaat noodzakelijk wordt geacht en een wettelijke verplichting wordt, zijn strengere controles en sancties gerechtvaardigd.

Niettemin kan de Koning, indien nodig, op initiatief van die overheid beslissen haar dezelfde toezichts- en sanctiebevoegdheden toe te kennen als die van de nationale cyberbeveiligingscertificeringsautoriteit, alsook dezelfde beroepsmogelijkheden, die in hoofdstuk 5 en 6 van de wet zijn vastgelegd voor vrijwillige certificeringen.

En effet, les autorités publiques qui souhaiteraient rendre obligatoire l'obtention d'un certificat de cybersécurité et qui ne bénéficieraient pas déjà de dispositions similaires en matière de contrôle et de sanction dans leurs lois sectorielles pourraient ainsi appliquer les chapitres 5 et 6 de la présente loi.

Conformément à l'article 1, § 2, du Règlement sur la cybersécurité et à l'article 4, § 2, du Traité sur l'Union européenne, la présente loi ne porte pas préjudice à l'adoption de mesures nationales en matière de certification de cybersécurité pour protéger la sécurité publique, la défense, la sécurité nationale et les activités dans le domaine du droit pénal.

De plus, le paragraphe 3 rappelle que la présente loi est sans préjudice des compétences des autorités publiques, notamment les autorités de surveillance de marché et les autorités sectorielles, de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle ainsi que, le cas échéant, les sanctions, en vertu de leurs compétences légales comme autorité de surveillance de marché, 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 (ci-après, la "loi NIS"), de la loi du 1er juillet 2011 relative à la protection et la sécurité des infrastructures critiques et de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

En tout état de cause, les autorités de surveillance de marché et les autorités sectorielles devront disposer des moyens humains et budgétaires suffisants pour contrôler les certifications obligatoires.

Par ailleurs, un quatrième paragraphe exclut l'application des paragraphes 2 à 4 de l'article 5 à la Banque nationale de Belgique visée par la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, à la FSMA visée par la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ainsi qu'au Service Public Fédéral Économie visé au Code de droit économique. Les paragraphes 2 et 3 de l'article 5 habilitent le Roi à confier, sous certaines conditions, à d'autres autorités administratives ou autorités administratives indépendantes que l'autorité nationale de certification de cybersécurité, des missions de contrôle normalement dévolues à cette dernière. Le paragraphe 4 prévoit que ces entités disposent des mêmes droits et obligations que celles de l'autorité nationale de certification de cybersécurité, sans préjudice de leurs compétences légales existantes.

Overheden die het verkrijgen van een cyberbeveiligingscertificaat verplicht willen maken en waarvan de sectorale wetten nog geen soortgelijke bepalingen inzake toezicht en sancties bevatten, kunnen zo immers hoofdstuk 5 en 6 van deze wet toepassen.

Overeenkomstig artikel 1, lid 2, van de Cyberbeveiligingsverordening en artikel 4, lid 2, van het Verdrag betreffende de Europese Unie doet deze wet geen afbreuk aan nationale maatregelen inzake cyberbeveiligingscertificering die worden genomen ter bescherming van de openbare veiligheid, defensie, de nationale veiligheid en de activiteiten op het gebied van het strafrecht.

Bovendien herinnert paragraaf 3 eraan dat deze wet geen afbreuk doet aan de bevoegdheden van de overheden, met name de markttoezichtautoriteiten en sectorale overheden, om een cyberbeveiligingscertificering op te leggen en te zorgen voor het toezicht op en, in voorkomend geval, de sancties met betrekking tot deze certificering, krachtens hun wettelijke bevoegdheden als markttoezichtautoriteit, 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 (hierna de "NIS-wet"), de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

De markttoezichtautoriteiten en sectorale overheden moeten in ieder geval over voldoende menselijke en budgettaire middelen beschikken om de verplichte certificeringen te controleren.

Voorts sluit een vierde paragraaf uit dat de paragrafen 2 tot 4 van artikel 5 worden toegepast 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, op de FSMA bedoeld in de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten en op de Federale Overheidsdienst Economie bedoeld in het Wetboek van economisch recht. De paragrafen 2 en 3 van artikel 5 machtigen de Koning om, onder bepaalde voorwaarden, toezichtsopdrachten waarmee normaal de nationale cyberbeveiligingscertificeringsautoriteit belast is, toe te vertrouwen aan andere administratieve overheden of onafhankelijke administratieve overheden. Paragraaf 4 bepaalt dat deze entiteiten dezelfde rechten en verplichtingen hebben als de nationale cyberbeveiligingscertificeringsautoriteit, onverminderd hun bestaande wettelijke bevoegdheden.

Cette exclusion s'explique par le fait que de nouvelles dispositions sont insérées dans les lois organiques de la Banque nationale de Belgique, de la FSMA ainsi que dans le Code de droit économique.

Enfin, le dernier paragraphe souligne que la loi n'a pas pour vocation de modifier les compétences de l'autorité nationale d'accréditation et les règles liées au système d'accréditation prévues par l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.

Section 2

Définitions

Art. 4

L'article 4 donne quelques définitions utiles pour le projet de loi.

La notion d'autorité publique vise de manière large toutes les autorités publiques du pays et reprend à cet effet la définition de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

CHAPITRE 2

Autorités compétentes et coopération au niveau national

Section 1re

Autorités compétentes

Art. 5

L'article 58 du Règlement sur la cybersécurité impose à chaque État membre de désigner une ou plusieurs autorités nationales de certification de cybersécurité sur son territoire. Le projet de loi dispose que le Roi désigne une seule autorité qui sera chargée, en tant qu'autorité nationale de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et la présente loi.

La désignation d'une seule autorité nationale de certification de cybersécurité est recommandée afin de faciliter pour tous les acteurs intéressés (fabricants, fournisseurs de services, organismes d'évaluation de la conformité, consommateurs, États membres de l'Union européenne,

Deze uitsluiting wordt verklaard door het feit dat nieuwe bepalingen worden ingevoegd in de organieke wetten van de Nationale Bank van België en de FSMA, alsook in het Wetboek van economisch recht.

Tot slot wijst de laatste paragraaf erop dat het niet de bedoeling van de wet is om de bevoegdheden van de nationale accreditatieautoriteit en de regels voor het accreditatiesysteem bepaald in het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling te wijzigen.

Afdeling 2

Definities

Art. 4

Artikel 4 bevat enkele nuttige definities voor het wetsontwerp.

Het begrip "overheid" heeft, in ruime zin, betrekking op alle overheden van het land en neemt hiervoor de definitie over van artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

HOOFDSTUK 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

Afdeling 1

Bevoegde autoriteiten

Art. 5

Artikel 58 van de Cyberbeveiligingsverordening verplicht elke lidstaat om een of meer nationale cyberbeveiligingscertificeringsautoriteiten op zijn grondgebied aan te wijzen. Het wetsontwerp bepaalt dat de Koning één autoriteit aanwijst die, als nationale cyberbeveiligingscertificeringsautoriteit, belast is met de taken en opdrachten bedoeld in de Cyberbeveiligingsverordening en in deze wet.

De aanwijzing van één nationale cyberbeveiligingscertificeringsautoriteit wordt aanbevolen om alle belanghebbenden (fabrikanten, dienstverleners, conformiteitsbeoordelingsinstanties, consumenten, lidstaten van de Europese Unie, enz.) gemakkelijker toegang te

etc.) l'accès aux informations nécessaires sur la certification de cybersécurité en Belgique.

D'un point de vue organisationnel, il est également souhaitable qu'une seule autorité centrale garde une vue d'ensemble des différents schémas de certification en matière de cybersécurité. Cela est d'autant plus vrai que l'on ne sait pas exactement quels schémas de certification l'Union européenne mettra en place à l'avenir, ni à quels types de produits, services ou processus ils s'appliqueront.

Lors de cette désignation, le Roi tiendra compte de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique ("CCB") qui confie au CCB les missions légales suivantes: coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication, coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière.

En vertu de l'article 60 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 (loi NIS) et de son arrêté d'exécution du 12 juillet 2019, le CCB assume également le rôle de centre national de réponse aux incidents de sécurité informatique ("CSIRT national").

Toutefois, le second paragraphe prévoit, à titre dérogatoire, que le Roi peut, par arrêté délibéré en Conseil des ministres, en fonction de l'objet du schéma de certification et à la demande d'une autre autorité publique, attribuer certaines missions de l'autorité nationale de certification de cybersécurité, en matière de contrôle (chapitre 5) et de sanctions (chapitre 6), à l'exception des articles 21 et 22, à cette autre autorité publique.

L'objectif n'est pas que le Roi attribue les tâches de contrôle et de sanction de l'autorité nationale de certification de cybersécurité pour toutes les certifications à d'autres administrations mais de permettre, via une éventuelle décision du Roi prise en concertation avec l'administration concernée et l'autorité nationale de certification de cybersécurité, de confier légalement les tâches de contrôle et de sanction dans le cadre de la présente loi à une autre administration en raison de son expertise particulière par rapport au schéma de certification concerné. Il ne s'agit toutefois ici que d'une faculté pour le Roi afin d'éviter des doublons dans les inspections et d'assurer une coordination dans les contrôles. À cette occasion, le Roi veille à respecter les répartitions de compétences existantes prévues par la

verlenen tot de nodige informatie over cyberbeveiligingscertificering in België.

Uit organisatorisch oogpunt is het ook wenselijk dat één centrale autoriteit het overzicht behoudt van de verschillende cyberbeveiligingscertificeringsregelingen, te meer daar men niet precies weet welke certificeringsregelingen de Europese Unie in de toekomst zal invoeren, noch op welke soorten producten, diensten of processen deze van toepassing zullen zijn.

Bij deze aanwijzing houdt de Koning rekening met het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België ("CCB"), dat het CCB de volgende wettelijke opdrachten toevertrouwt: coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen, coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak.

Krachtens artikel 60 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 (NIS-wet) en het bijhorende uitvoeringsbesluit van 12 juli 2019 vervult het CCB ook de rol van nationaal computer security incident response team ("nationaal CSIRT").

Bij wijze van afwijking bepaalt de tweede paragraaf echter dat de Koning, bij besluit vastgesteld na overleg in de Ministerraad, naargelang het voorwerp van de certificeringsregeling en op verzoek van een andere overheid, bepaalde opdrachten van de nationale cyberbeveiligingscertificeringsautoriteit inzake toezicht (hoofdstuk 5) en sancties (hoofdstuk 6), met uitzondering van artikel 21 en 22, kan toewijzen aan deze andere overheid.

Het is niet de bedoeling dat de Koning de taken inzake toezicht en sancties van de nationale cyberbeveiligingscertificeringsautoriteit voor alle certificeringen aan andere administraties toewijst, maar dat, via een eventuele beslissing van de Koning genomen in overleg met de betrokken administratie en de nationale cyberbeveiligingscertificeringsautoriteit, de taken inzake toezicht en sancties in het kader van deze wet wettelijk kunnen worden toevertrouwd aan een andere administratie vanwege haar bijzondere expertise in verband met de betrokken certificeringsregeling. Het betreft hier echter alleen een mogelijkheid voor de Koning teneinde dubbel inspectiewerk te voorkomen en ervoor te zorgen dat de controles gecoördineerd gebeuren. Bij deze gelegenheid ziet de Koning toe op de naleving van de in de wet

loi. Il veille ainsi notamment à ce que les compétences de l'autorité qu'il charge d'assurer le contrôle en ce qui concerne une certification de cybersécurité s'étendent uniquement aux entreprises qui tombent déjà dans le champ des compétences de l'autorité concernée. Par ailleurs, le Roi veille à tenir compte de l'expertise de l'autorité concernée lors de l'attribution éventuelle de tâches de contrôle.

Conformément aux articles 58, § 5, et 59, § 2, du Règlement sur la cybersécurité, toute autorité publique qui doit assurer des missions de contrôle doit disposer des moyens humains et budgétaires suffisants pour réaliser ses tâches.

Le troisième paragraphe précise que le Roi doit, préalablement au fait de confier certaines tâches de contrôle à une autre autorité, se concerter avec celle-ci.

Par ailleurs, le quatrième paragraphe prévoit que ces entités, auxquelles auront été attribuées certaines compétences de l'autorité nationale de certification de cybersécurité, disposent des mêmes droits et obligations que celles de l'autorité nationale de certification de cybersécurité visées au chapitre 5, sans préjudice de leurs compétences légales existantes. Cette disposition garantit le respect du principe d'égalité et de non-discrimination en imposant le respect des mêmes obligations à toute entité à laquelle serait attribuée une ou plusieurs compétences dévolues, en principe, à l'autorité nationale de certification de cybersécurité en vertu du Règlement sur la cybersécurité ou de la présente loi.

Section 2

Coopération au niveau national

Art. 6

Cet article énonce que l'autorité nationale de certification de cybersécurité ou l'autorité visée à l'article 5, § 2 se concerte avec les autres autorités publiques, notamment avec l'autorité nationale d'accréditation. Il permet également à l'autorité nationale de certification de cybersécurité ou à l'autorité visée à l'article 5, § 2 de consulter, par exemple, les fédérations professionnelles concernées par la certification en matière de cybersécurité.

Le Règlement sur la cybersécurité prévoit notamment, en son article 58, § 7, h), que l'autorité nationale de certification de cybersécurité coopère, non seulement avec les autres autorités nationales de certification de cybersécurité, mais également avec d'autres autorités publiques. Ces autorités se partagent notamment, au

bepaalde bestaande bevoegdheidsverdelingen. Hij zorgt er met name voor dat de bevoegdheden van de overheid die Hij belast met het toezicht in verband met een cyberbeveiligingscertificering, enkel betrekking hebben op ondernemingen die al onder de bevoegdheid van de betrokken overheid vallen. Verder houdt de Koning rekening met de expertise van de betrokken overheid bij de eventuele toekenning van toezichtstaken.

Overeenkomstig de artikelen 58, lid 5, en 59, lid 2, van de Cyberbeveiligingsverordening moet elke overheid die toezichtsopdrachten vervult over voldoende menselijke en budgettaire middelen beschikken om haar taken uit te voeren.

Volgens de derde paragraaf moet de Koning, alvorens bepaalde toezichtstaken toe te vertrouwen aan een andere overheid, overleg plegen met die laatste.

Voorts bepaalt de vierde paragraaf dat deze entiteiten, waaraan bepaalde bevoegdheden van de nationale cyberbeveiligingscertificeringsautoriteit zijn toegekend, dezelfde rechten en verplichtingen hebben als die van de nationale cyberbeveiligingscertificeringsautoriteit bedoeld in hoofdstuk 5, onverminderd hun bestaande wettelijke bevoegdheden. Deze bepaling waarborgt de naleving van het gelijkheids- en non-discriminatiebeginsel door dezelfde verplichtingen op te leggen aan elke entiteit waaraan een of meer bevoegdheden worden toegekend waarover de nationale cyberbeveiligingscertificeringsautoriteit in beginsel krachtens de Cyberbeveiligingsverordening of deze wet beschikt.

Afdeling 2

Samenwerking op nationaal niveau

Art. 6

Dit artikel vermeldt dat de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2, overleg pleegt met de andere overheden, met name met de nationale accreditatieautoriteit. Het laat de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in 5, § 2, ook toe om bijvoorbeeld de beroepsfederaties te raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.

Artikel 58, lid 7, onder h), van de Cyberbeveiligingsverordening bepaalt met name dat de nationale cyberbeveiligingscertificeringsautoriteit niet alleen samenwerkt met andere nationale cyberbeveiligingscertificeringautoriteiten, maar ook met andere overheden. Via deze samenwerking wisselen deze

travers de cette coopération, des informations en matière de contrôle du respect des exigences dudit règlement et du schéma de certification de cybersécurité.

Conformément au paragraphe 2, l'autorité nationale de certification de cybersécurité et les autres autorités publiques visées par ce paragraphe pourront s'échanger mutuellement toutes les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ainsi qu'aux 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 sanction et de réclamation. Les articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques portent sur la sécurité des communications électroniques. Ces dispositions permettent aux opérateurs de prendre des mesures adéquates pour gérer les risques pour la sécurité de leurs réseaux et services. Elles permettent également à l'Institut belge des services postaux et des télécommunications d'imposer des mesures et de contrôler le respect de ces mesures auprès des opérateurs.

Pour rappel, le Règlement sur la cybersécurité définit la cybersécurité comme "les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces". Les articles 107/2 à 107/5 constituent, en ce sens, des dispositions portant directement sur la cybersécurité et octroyant, à l'Institut belge des services postaux et des télécommunications, des compétences en matière de cybersécurité.

Dès lors, conformément à ce que préconise l'Autorité de protection des données dans son avis n° 08/2022 du 21 janvier 2022 (voir les points 9, 11 et 13 de l'avis), il est possible de prévoir, dans le projet de loi, un échange d'informations pouvant porter sur des données à caractère personnel.

Ce partage d'information demeure néanmoins limité à ce qui est pertinent et proportionné à l'objectif de cet échange, notamment dans le respect d'autres dispositions légales nationales ou internationales.

Si la collaboration conduit à une transmission de données à caractère personnel entre autorités, il sera tenu compte des dispositions applicables à la protection des données à caractère personnel et notamment 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, des principes du Règlement (UE) 2016/679 (règlement général sur la protection des données), notamment la limitation du

overheden met name informatie uit over het toezicht op de naleving van de voorschriften van deze verordening en van de cyberbeveiligingscertificeringsregeling.

Overeenkomstig paragraaf 2 kunnen de nationale cyberbeveiligingscertificeringsautoriteit en de andere overheden bedoeld in deze paragraaf onderling alle informatie uitwisselen die nodig is voor de toepassing van de Cyberbeveiligingsverordening, deze wet en 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. De artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie hebben betrekking op de veiligheid van elektronische communicatie. Krachtens deze bepalingen kunnen operatoren passende maatregelen nemen om de risico's voor de veiligheid van hun netwerken en diensten te beheersen en kan het Belgisch Instituut voor postdiensten en telecommunicatie maatregelen opleggen en toezien op de naleving ervan door de operatoren.

Ter herinnering: de Cyberbeveiligingsverordening definieert cyberbeveiliging als "de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen". In die zin zijn de artikelen 107/2 tot 107/5 bepalingen die rechtstreeks betrekking hebben op cyberbeveiliging en die het Belgisch Instituut voor postdiensten en telecommunicatie bevoegdheden inzake cyberbeveiliging toekennen.

Zoals de Gegevensbeschermingsautoriteit in haar advies nr. 08/2022 van 21 januari 2022 aanbeveelt (zie punt 9, 11 en 13 van het advies), maakt het wetsontwerp bijgevolg informatie-uitwisseling mogelijk die persoonsgegevens kan betreffen.

Deze informatie-uitwisseling blijft evenwel beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig andere nationale of internationale wettelijke bepalingen.

Indien de samenwerking leidt tot een overdracht van persoonsgegevens tussen overheden, wordt rekening gehouden met de bepalingen die van toepassing zijn op de bescherming van persoonsgegevens en met name met artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, met de beginselen van Verordening (EU) 2016/679 (algemene verordening gegevensbescherming), met name de

traitement à ce qui est nécessaire en vue de l'objectif poursuivi, ainsi que des dispositions du chapitre 8.

En matière d'échange d'informations, le troisième paragraphe permet, plus spécifiquement, à l'autorité nationale de certification de cybersécurité ou aux autorités visées à l'article 5, § 2, de la loi de communiquer toute information obtenue dans le cadre de l'exécution du Règlement sur la cybersécurité ou de la présente loi, aux autorités sectorielles, aux services d'inspection, à l'inspection aéroportuaire, à l'inspection aéronautique et à la "Belgian Supervising Authority for Air Navigation Services" (ci-après, la "BSA-ANS") visés à la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, la loi NIS ou à l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Les informations dont il est question doivent respecter les autres dispositions de la présente loi. Notamment, la communication d'information prévue au paragraphe 3 n'est opérée qu'auprès des autorités compétentes pour le contrôle de l'entité concernée et ne peut porter sur les données à caractère personnel des clients (ou des données à caractère personnel traitées par ces derniers) des titulaires de certificats de cybersécurité ou des émetteurs de déclarations de conformité contrôlés. En tous les cas, lorsque l'information communiquée contient des données à caractère personnel, elle est soumise aux dispositions du chapitre 8 relatives au traitement de ce type de données.

L'existence de cette communication s'explique de par les compétences, en matière de cybersécurité, que détiennent les autorités citées.

En effet, selon l'article 7, § 3, de la loi NIS, les autorités sectorielles ont pour mission de veiller à la mise en œuvre de la loi précitée. Pour ce faire, elles sont accompagnées de services d'inspection qui, conformément à l'article 7, § 5, de la loi NIS, sont chargés du contrôle du respect des dispositions de cette même loi. À ce titre, ces autorités s'assurent que les entités soumises à la loi NIS adoptent les mesures de sécurité nécessaires pour gérer les risques menaçant la sécurité des réseaux et systèmes d'information dont leurs services essentiels sont tributaires (articles 20 et 33 de la loi NIS) et élaborent une politique de sécurité de leurs systèmes et réseaux d'information (article 21, § 1er, de la loi NIS). Conformément à l'article 24, § 1er, de la loi du 1 juillet 2011 relative à la sécurité et la protection des infrastructures critiques (ci-après, la "loi IC"), les services d'inspection établis par cette loi sont chargés du contrôle du respect des dispositions de la présente loi. A ce titre, les services d'inspection s'assurent que les plans de

beperking van de verwerking tot hetgeen noodzakelijk is voor het nagestreefde doel, alsook met de bepalingen van hoofdstuk 8.

Wat informatie-uitwisseling betreft, bepaalt de derde paragraaf met name dat de nationale cyberbeveiligingscertificeringsautoriteit of de overheden bedoeld in artikel 5, § 2, van de wet alle informatie verkregen in het kader van de uitvoering van de Cyberbeveiligingsverordening of van deze wet kunnen meedelen aan de sectorale overheden, de inspectiediensten, de luchthaveninspectie, de luchtvaartinspectie en de "Belgian Supervising Authority for Air Navigation Services" (hierna de "BSA-ANS"), als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de NIS-wet of het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

De betrokken informatie moet voldoen aan de overige bepalingen van deze wet. De in paragraaf 3 bedoelde informatie wordt met name alleen meegedeeld aan overheden die bevoegd zijn voor het toezicht op de betrokken entiteit en mag geen betrekking hebben op persoonsgegevens van klanten (of persoonsgegevens die laatstgenoemden verwerken) van gecontroleerde houders van cyberbeveiligingscertificaten of afgevers van conformiteitsverklaringen. Indien de meegedeelde informatie persoonsgegevens bevat, is ze in ieder geval onderworpen aan de bepalingen van hoofdstuk 8 betreffende de verwerking van dit soort gegevens.

Het bestaan van deze mededeling is te verklaren in het licht van de bevoegdheden inzake cyberbeveiliging van de vermelde overheden.

Volgens artikel 7, § 3, van de NIS-wet hebben de sectorale overheden immers als opdracht toe te zien op de uitvoering van voornoemde wet. Daartoe worden zij bijgestaan door inspectiediensten die, overeenkomstig artikel 7, § 5, van de NIS-wet, toezien op de naleving van de bepalingen van dezelfde wet. In dit verband zorgen deze overheden ervoor dat entiteiten die onderworpen zijn aan de NIS-wet, passende beveiligingsmaatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan hun essentiële diensten afhankelijk zijn, te beheersen (artikel 20 en 33 van de NIS-wet), en een beveiligingsbeleid uitwerken voor hun netwerk- en informatiesystemen (artikel 21, § 1, van de NIS-wet). Overeenkomstig artikel 24, § 1, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (hierna de "KI-wet") zijn de bij deze wet ingestelde inspectiediensten belast met de controle op de naleving van de bepalingen van deze wet. In dit verband zorgen de inspectiediensten

sécurité de l'exploitant, visés à l'article 13 de la loi IC, sont respectés. Enfin, selon les articles 11 et 15 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien et les 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 sectorielle, le service d'inspection, l'inspection aéroportuaire, l'inspection aéronautique et la BSA-ANS, visés 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, sont compétents pour superviser le respect des plans de sécurité de l'exploitant, visés à l'article 13 de la loi IC, ainsi que des dispositions relatives à la sécurité des données et systèmes de technologies de l'information et de la communication 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.

La publicité des retraits de certificats de cybersécurité européens, évoquée par l'Autorité de protection des données dans son avis n° 08/2022 du 21 janvier 2022, au point 12, n'est pas suffisante pour remplacer l'échange d'information prévu au présent paragraphe car les informations visées par cette disposition ne se retrouveront pas forcément au sein des décisions de retrait. Notamment, les informations relatives à l'octroi, ou au refus d'octroi, d'un certificat de cybersécurité européen dont l'obtention fait partie d'une politique de sécurité des systèmes et réseaux d'information (P.S.I.), d'un plan de sécurité de l'exploitant (P.S.E.) ou des mesures de protection ou de sécurité nécessaires de l'entité soumise à la supervision d'une des entités précitées ne sont pas couvertes par la publicité des décisions de retraits de certificats.

Lorsqu'un certificat de cybersécurité européen ou une déclaration de conformité constitue une mesure de protection ou de sécurité nécessaire ou, le cas échéant, reprise à la P.S.I. ou au P.S.E. de l'entité concernée, il apparaît nécessaire de pouvoir fournir toute information relative à ce certificat ou cette déclaration, constituant une violation de la loi NIS, à l'autorité sectorielle et au service d'inspection concernés.

Cette disposition ne porte pas sur les rapports et procès-verbaux du service d'inspection, qui font l'objet

ervoor dat de beveiligingsplannen van de exploitant, als bedoeld in artikel 13 van de KI-wet, worden nageleefd. En tot slot: volgens artikel 11 en 15 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en afdeling 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 zijn de sectorale overheid, de inspectiedienst, de luchthaveninspectie, de luchtvaartinspectie en de BSA-ANS, als bedoeld 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, bevoegd om toe te zien op de naleving van de beveiligingsplannen van de exploitant, als bedoeld in artikel 13 van de KI-wet, en van de bepalingen betreffende de beveiliging van gegevens en informatie- en communicatiesystemen in 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.

De openbaarmaking van intrekkingen van Europese cyberbeveiligingscertificaten, waarnaar de Gegevensbeschermingsautoriteit in punt 12 van haar advies nr. 08/2022 van 21 januari 2022 verwijst, volstaat niet om de in deze paragraaf bedoelde informatie-uitwisseling te vervangen, aangezien de in deze bepaling bedoelde informatie niet noodzakelijkerwijs vermeld zal zijn in de intrekkingsbeslissingen. Informatie over de toekenning of weigering tot toekenning van een Europees cyberbeveiligingscertificaat dat moet worden behaald als deel van een beveiligingsbeleid voor de netwerk- en informatiesystemen (IBB), van een beveiligingsplan van de exploitant (BPE) of van noodzakelijke beschermings- of beveiligingsmaatregelen van de entiteit die onder het toezicht van een van voornoemde entiteiten staat, valt met name niet onder de openbaarmaking van beslissingen tot intrekking van certificaten.

Indien een Europees cyberbeveiligingscertificaat of een conformiteitsverklaring een beschermings- of beveiligingsmaatregel is die noodzakelijk is of, in voorkomend geval, deel uitmaakt van het IBB of BPE van de betrokken entiteit, moet alle informatie over dit certificaat of deze verklaring die een schending van de NIS-wet inhoudt, kunnen worden verstrekt aan de betrokken sectorale overheid en inspectiedienst.

Deze bepaling heeft geen betrekking op verslagen en processen-verbaal van de inspectiedienst, waarvoor

de dispositions spécifiques (voir *infra*, les commentaires des articles 16 et 17).

Le paragraphe 4 autorise les autorités publiques soumises au secret professionnel à transmettre les informations soumises à ce secret à l'autorité nationale de certification de cybersécurité ou aux autorités visées à l'article 5, § 2 lorsque cela est nécessaire à l'application de la présente loi ou du Règlement sur la cybersécurité.

Bien entendu, cette disposition ne porte pas préjudice à l'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Il s'agit d'un régime juridique distinct de celui du secret professionnel. Ce paragraphe ne permet donc pas de s'affranchir du respect des obligations légales relatives aux traitements d'éventuelles informations classifiées. Par ailleurs, lorsque les informations visées par cette disposition portent sur des données à caractère personnel, les dispositions du chapitre 8 s'appliquent.

Cette disposition ne s'applique pas aux professionnels soumis au secret professionnel, tels que les avocats et les médecins. Une disposition spécifique, prévue à l'article 15, § 9, de la présente loi, s'applique à ces derniers.

Art. 7

Sauf attribution par le Roi de certaines missions de contrôle à une autre autorité, le contrôle des certifications volontaires de cybersécurité est assuré par l'autorité nationale de certification de cybersécurité. Sur base de cet article, l'autorité nationale de certification de cybersécurité ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 peut éventuellement solliciter la collaboration d'une autre autorité qui agirait dans le cadre de ses propres compétences légales de contrôle, afin de l'assister dans ses missions de contrôle.

specifieke bepalingen gelden (zie hieronder de commentaar bij de artikelen 16 en 17).

Paragraaf 4 zorgt ervoor dat overheden die gebonden zijn aan het beroepsgeheim informatie die hieronder valt, kunnen overmaken aan de nationale cyberbeveiligingscertificeringsautoriteit of de overheden bedoeld in artikel 5, § 2, indien dit nodig is voor de toepassing van deze wet of van de Cyberbeveiligingsverordening.

Uiteraard doet deze bepaling geen afbreuk aan de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Het betreft een andere juridische regeling dan die van het beroepsgeheim. Deze paragraaf laat dus niet toe de wettelijke verplichtingen met betrekking tot de verwerking van eventuele geclassificeerde informatie te veronachtzamen. Indien de informatie bedoeld in deze bepaling persoonsgegevens betreft, zijn de bepalingen van hoofdstuk 8 overigens van toepassing.

Deze bepaling is niet van toepassing op beroepsbeoefenaars die onder het beroepsgeheim vallen, zoals advocaten en artsen. Voor laatstgenoemden geldt een specifieke bepaling in artikel 15, § 9, van deze wet.

Art. 7

Tenzij de Koning bepaalde toezichtsopdrachten aan een andere overheid heeft toegewezen, wordt het toezicht op de vrijwillige cyberbeveiligingscertificeringen uitgeoefend door de nationale cyberbeveiligingscertificeringsautoriteit. Op basis van dit artikel kan de nationale cyberbeveiligingscertificeringsautoriteit of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, eventueel een andere overheid verzoeken om haar voor haar toezichtsopdrachten bij te staan, en dit in het kader van de eigen wettelijke toezichtsbevoegdheden van laatstgenoemde.

CHAPITRE 3

Autorité nationale de certification de cybersécurité

Section 1re

Représentation au Groupe européen de certification de cybersécurité

Art. 8

L'article précise que l'autorité nationale de certification de cybersécurité représentera la Belgique au sein du Groupe européen de certification de cybersécurité (ci-après "GECC") visé à l'article 62 du Règlement sur la cybersécurité. Le GECC est chargé notamment de conseiller et d'assister la Commission en matière de certification de cybersécurité, d'adopter un avis sur les schémas candidats préparés par l'ENISA (l'agence européenne chargé de la cybersécurité), de demander à l'ENISA de préparer un schéma candidat et de faciliter la coopération entre les autorités nationales de certification de cybersécurité.

Lors des discussions relatives à l'adoption d'actes d'exécution liés au Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité représentera également la Belgique au cours des réunions visées par le Règlement n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission.

Les schémas européens de certification de cybersécurité ont vocation à contribuer à harmoniser les pratiques de cybersécurité au sein de l'Union. Ils doivent contribuer à augmenter le niveau de cybersécurité dans l'Union. La conception des schémas européens de certification de cybersécurité devrait également prendre en compte et permettre la mise au point d'innovations dans le domaine de la cybersécurité.

Le deuxième paragraphe souligne que dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité nationale de certification de cybersécurité se concertera avec les autres autorités publiques concernées (désignées par le Roi), en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma candidat de certification de cybersécurité.

Il est, en effet, souhaitable que l'autorité nationale de certification de cybersécurité se concerte au préalable notamment avec les différentes autorités de surveillance

HOOFDSTUK 3

Nationale cyberbeveiligingscertificeringsautoriteit

Afdeling 1

Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering

Art. 8

Volgens dit artikel zal de nationale cyberbeveiligingscertificeringsautoriteit België vertegenwoordigen in de Europese Groep voor cyberbeveiligingscertificering (hierna "EGC") bedoeld in artikel 62 van de Cyberbeveiligingsverordening. De EGC heeft met name als taak advies en bijstand te verlenen aan de Commissie op het vlak van cyberbeveiligingscertificering, een advies uit te brengen over potentiële regelingen opgesteld door ENISA (het Europees agentschap voor cyberbeveiliging), ENISA te verzoeken potentiële regelingen op te stellen en de samenwerking tussen de nationale cyberbeveiligingscertificeringsautoriteiten te vergemakkelijken.

De nationale cyberbeveiligingscertificeringsautoriteit zal België ook vertegenwoordigen tijdens besprekingen voor de vaststelling van uitvoeringshandelingen in verband met de Cyberbeveiligingsverordening op de vergaderingen bedoeld in Verordening nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren.

Met Europese cyberbeveiligingscertificeringsregelingen wordt beoogd bij te dragen aan de harmonisatie van cyberbeveiligingspraktijken in de Unie. Zij dienen bij te dragen tot een betere cyberbeveiliging binnen de Unie. Bij het ontwerp van de Europese cyberbeveiligingscertificeringsregelingen moet de ontwikkeling van innovaties op het gebied van cyberbeveiliging in aanmerking worden genomen en mogelijk zijn.

De tweede paragraaf wijst erop dat de nationale cyberbeveiligingscertificeringsautoriteit, in het kader van haar opdracht om België in de EGC te vertegenwoordigen, met de andere betrokken (door de Koning aangewezen) overheden overlegt, met name bij de voorbereiding en goedkeuring van een advies over een potentiële cyberbeveiligingscertificeringsregeling.

Het is immers wenselijk dat de nationale cyberbeveiligingscertificeringsautoriteit vooraf met name met de verschillende markttoezichtautoriteiten, de sectorale

du marché, les autorités sectorielles visées par la loi NIS, les entités fédérées ou d'autres autorités publiques qui pourraient être concernées par le schéma de certification européen proposé.

La variété des objets sur lesquels pourront porter les propositions de schémas européens de certification de cybersécurité requiert, en outre, une structure flexible de concertation avec les acteurs concernés au niveau national, en fonction de chaque schéma précis.

De plus, le paragraphe 3 prévoit que ces autres autorités publiques pourront assister avec l'autorité nationale de certification de cybersécurité aux travaux et réunions du GECC.

Section 2

Indépendance

Art. 9

Cet article met en œuvre l'article 58, § 3, du Règlement sur la cybersécurité qui impose que chaque autorité nationale de certification de cybersécurité soit indépendante des entités qu'elle surveille en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel.

La disposition précise les situations de conflits d'intérêts que l'autorité nationale de certification de cybersécurité doit prévenir, identifier et résoudre lors de l'exécution de ses tâches de contrôle et de certification en matière de cybersécurité.

CHAPITRE 4

Délivrance des certificats européens

Section 1re

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élémentaire" ou "substantiel"

Art. 10

En vertu de l'article 56, § 4, du Règlement sur la cybersécurité, les organismes d'évaluation de la conformité accrédités délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel".

Les schémas européens de certification de cybersécurité auront pour finalité de garantir que les produits

overheden bedoeld in de NIS-wet, de deelgebieden of andere overheden overlegt die betrokken kunnen zijn bij de voorgestelde Europese certificeringsregeling.

De verscheidenheid van de zaken waarop voorstellen voor Europese cyberbeveiligingscertificeringsregelingen betrekking kunnen hebben, vereist bovendien een flexibele structuur voor het overleg met de betrokkenen op nationaal niveau, naargelang elke specifieke regeling.

Verder bepaalt paragraaf 3 dat deze andere overheden, samen met de nationale cyberbeveiligingscertificeringsautoriteit, de werkzaamheden en vergaderingen van de EGC kunnen bijwonen.

Afdeling 2

Onafhankelijkheid

Art. 9

Dit artikel geeft uitvoering aan artikel 58, lid 3, van de Cyberbeveiligingsverordening waaruit blijkt dat elke nationale cyberbeveiligingscertificeringsautoriteit op het vlak van haar organisatie, financieringsbeslissingen, rechtsstructuur en besluitvorming onafhankelijk moet zijn van de entiteiten waarop zij toezicht houdt.

De bepaling verduidelijkt welke situaties van belangenconflicten de nationale cyberbeveiligingscertificeringsautoriteit moet voorkomen, identificeren en oplossen bij de uitvoering van haar toezichts- en certificeringstaken op het gebied van cyberbeveiliging.

HOOFDSTUK 4

Afgifte van Europese certificaten

Afdeling 1

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"

Art. 10

Krachtens artikel 56, lid 4, van de Cyberbeveiligingsverordening geven de geaccrediteerde conformiteitsbeoordelingsinstanties de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af.

Europese cyberbeveiligingscertificeringsregelingen moeten tot doel hebben te waarborgen dat ICT-producten,

TIC, services TIC et processus TIC certifiés selon de tels schémas respectent les exigences définies qui visent à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées, transmises ou traitées, ou des fonctions connexes de ces produits, services et processus tout au long de leur cycle de vie, ou des services qu'ils offrent ou qui sont accessibles par leur intermédiaire.

Comme le prévoit l'article 52, § 5, du Règlement sur la cybersécurité, le niveau d'assurance dit "élémentaire" offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificatif ou une déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques.

Quant au niveau d'assurance dit "substantiel", l'article 52, § 6, du Règlement sur la cybersécurité dispose qu'il offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées.

L'article 56, § 5, du même Règlement précise que la délivrance de tels certificats est néanmoins réservée à l'autorité nationale de certification de cybersécurité, lorsque le schéma de certification de cybersécurité l'exige. Pour ce faire et conformément à l'article 60, § 2, du Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité devra disposer d'une accréditation délivrée par l'organisme national d'accréditation. L'autorité nationale de certification de cybersécurité peut toutefois déléguer en tout ou en partie cette tâche à un organisme public accrédité en tant qu'organisme d'évaluation de la conformité.

L'éventuelle délégation prévue au troisième paragraphe est légalement admissible dès lors qu'elle n'octroie à l'organisme public accrédité en tant qu'organisme d'évaluation de la conformité aucun pouvoir réglementaire. De plus, cette délégation ne porte que sur une mission technique et spécifique, à savoir la délivrance de certificats de cybersécurité de niveau "élémentaire" ou "substantiel" sur base d'un schéma précis de certification européen.

-diensten en -processen die door middel van een dergelijke regeling zijn gecertificeerd, voldoen aan gespecificeerde voorschriften met als doel de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die producten, diensten en processen worden aangeboden of toegankelijk zijn, gedurende de levenscyclus ervan te beschermen.

Zoals bepaald in artikel 52, lid 5, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "basis" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat of EU-conformiteitsverklaring is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende basisrisico's van incidenten en cyberaanvallen tot een minimum te beperken.

Volgens artikel 52, lid 6, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "substantieel" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende cyberbeveiligingsrisico's, en het risico op incidenten en cyberaanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken.

Artikel 56, lid 5, van dezelfde Verordening verduidelijkt niettemin dat de afgifte van deze certificaten voorbehouden is aan de nationale cyberbeveiligingscertificeringsautoriteit indien de cyberbeveiligingscertificeringsregeling dit vereist. Overeenkomstig artikel 60, lid 2, van de Cyberbeveiligingsverordening moet de nationale cyberbeveiligingscertificeringsautoriteit daartoe beschikken over een accreditatie die wordt afgegeven door de nationale accreditatie-instantie. De nationale cyberbeveiligingscertificeringsautoriteit kan deze taak echter volledig of gedeeltelijk delegeren aan een overheidsinstelling die als conformiteitsbeoordelingsinstantie geaccrediteerd is.

De in de derde paragraaf bedoelde eventuele delegatie is wettelijk toegestaan, aangezien ze geen regelgevende bevoegdheid verleent aan de overheidsinstelling die als conformiteitsbeoordelingsinstantie geaccrediteerd is. Bovendien betreft deze delegatie alleen een technische en specifieke opdracht, namelijk de afgifte van cyberbeveiligingscertificaten voor niveau "basis" of "substantieel", op basis van een specifieke Europese certificeringsregeling.

Section 2

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élevé"

Art. 11

En vertu de l'article 56, § 6, du Règlement sur la cybersécurité, une certification européenne de cybersécurité d'un niveau d'assurance dit "élevé" ne peut être délivrée que par l'autorité nationale de certification de cybersécurité ou, éventuellement, en cas de délégation, par un organisme d'évaluation de la conformité. Conformément à l'article 60, § 2, du Règlement sur la cybersécurité, l'autorité nationale de certification de cybersécurité devra obtenir une accréditation auprès de l'organisme national d'accréditation.

Le projet énonce ainsi que l'autorité nationale de certification de cybersécurité délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé" ou, moyennant une délégation préalable de l'autorité nationale de certification de cybersécurité, un organisme accrédité d'évaluation de la conformité pourrait en tout ou en partie accomplir cette tâche.

L'article 56, § 7, du Règlement précise que l'autorité nationale de certification de cybersécurité ou l'organisme d'évaluation de la conformité peuvent obtenir de la personne physique ou morale sollicitant une certification toutes les informations nécessaires pour accorder celle-ci.

L'article 52, § 7, du Règlement sur la cybersécurité indique que le niveau d'assurance dit "élevé" offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels un certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes.

L'éventuelle délégation prévue au deuxième paragraphe est, au travers d'un raisonnement similaire à la délégation prévue à l'article 10, légalement admissible dès lors qu'elle n'octroie à l'organisme accrédité d'évaluation de la conformité aucun pouvoir réglementaire. De plus, cette délégation ne porte que sur une mission technique et spécifique, à savoir la délivrance de certificats de cybersécurité de niveau "haut". Cette mission exige une expertise particulière, l'intérêt de la présente délégation est de permettre à un organisme accrédité d'évaluation de la conformité possédant déjà cette expertise de s'en acquitter.

Afdeling 2

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"

Art. 11

Krachtens artikel 56, lid 6, van de Cyberbeveiligingsverordening kan een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "hoog" enkel worden afgegeven door de nationale cyberbeveiligingscertificeringsautoriteit of, eventueel in geval van delegatie, door een conformiteitsbeoordelingsinstantie. Overeenkomstig artikel 60, lid 2, van de Cyberbeveiligingsverordening moet de nationale cyberbeveiligingscertificeringsautoriteit door de nationale accreditatie-instantie worden geaccrediteerd.

Zo bepaalt het ontwerp dat de nationale cyberbeveiligingscertificeringsautoriteit de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" afgeeft, maar dat deze taak, na voorafgaande delegatie door de nationale cyberbeveiligingscertificeringsautoriteit, ook volledig of gedeeltelijk kan worden uitgevoerd door een geaccrediteerde conformiteitsbeoordelingsinstantie.

Artikel 56, lid 7, van de Verordening bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit of de conformiteitsbeoordelingsinstantie alle informatie kan verkrijgen van de natuurlijke of rechtspersoon die een certificering vraagt wanneer die nodig is om deze certificering te verlenen.

Volgens artikel 52, lid 7, van de Cyberbeveiligingsverordening biedt het zekerheidsniveau "hoog" de zekerheid dat de ICT-producten, -diensten en -processen waarvoor een certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken.

De eventuele delegatie bedoeld in de tweede paragraaf is, volgens een soortgelijke redenering als de delegatie in artikel 10, wettelijk toegestaan, aangezien ze geen regelgevende bevoegdheid verleent aan de geaccrediteerde conformiteitsbeoordelingsinstantie. Bovendien betreft deze delegatie slechts een technische en specifieke opdracht, namelijk de afgifte van cyberbeveiligingscertificaten voor niveau "hoog". Deze opdracht vereist een bijzondere expertise. Dankzij deze delegatie kan een geaccrediteerde conformiteitsbeoordelingsinstantie die al over deze expertise beschikt, deze opdracht uitvoeren.

Section 3

Réclamation en cas de refus de délivrance

Art. 12

Conformément à l'article 63, § 1er, du Règlement, les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité agissant conformément à l'article 56, § 6, auprès de l'autorité nationale de certification de cybersécurité concernée.

L'article 58, § 7, f), du Règlement confirme que l'autorité nationale de certification de cybersécurité est compétente pour traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par elle ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 56, § 6.

Sauf les hypothèses particulières précitées de compétence de l'autorité nationale de certification de cybersécurité, le refus de délivrance d'un certificat de niveau "élémentaire" ou "substantiel" peut donc être contesté directement par le demandeur auprès de l'organisme d'évaluation de la conformité concerné.

CHAPITRE 5

Contrôle

Ce chapitre énonce les règles relatives aux contrôles du respect par les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le Règlement sur la cybersécurité, la présente loi ou ses arrêtés d'exécution.

Art. 13

Cette disposition indique que l'autorité nationale de certification de cybersécurité ou l'autorité visée à l'article 5, § 2 doit disposer d'un service d'inspection capable, sans préjudice de l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de

Afdeling 3

Klacht ingeval de afgifte geweigerd wordt

Art. 12

Overeenkomstig artikel 63, lid 1, van de Verordening hebben natuurlijke en rechtspersonen het recht een klacht in te dienen bij de afgever van een Europees cyberbeveiligingscertificaat of, wanneer de klacht verband houdt met een Europees cyberbeveiligingscertificaat dat is afgegeven door een conformiteitsbeoordelingsinstantie handelend overeenkomstig artikel 56, lid 6, bij de bevoegde nationale cyberbeveiligingscertificeringsautoriteit.

Artikel 58, lid 7, onder f), van de Verordening bevestigt dat de nationale cyberbeveiligingscertificeringsautoriteit bevoegd is voor de behandeling van klachten van natuurlijke of rechtspersonen over door haar of overeenkomstig artikel 56, lid 6, door conformiteitsbeoordelingsinstanties afgegeven Europese cyberbeveiligingscertificaten.

Behalve in voornoemde specifieke gevallen waarin de nationale cyberbeveiligingscertificeringsautoriteit bevoegd is, kan de aanvrager de weigering om een certificaat voor niveau "basis" of "substantieel" af te geven dus rechtstreeks betwisten bij de bevoegde conformiteitsbeoordelingsinstantie.

HOOFDSTUK 5

Toezicht

Dit hoofdstuk bevat de regels over de controles om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de Cyberbeveiligingsverordening, deze wet of de uitvoeringsbesluiten ervan.

Art. 13

Volgens deze bepaling moet de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2, over een inspectiedienst beschikken die op elk ogenblik controles kan uitvoeren om na te gaan of de regels van de Cyberbeveiligingsverordening worden nageleefd, onverminderd de toepassing van het

la conformité, de réaliser à tout moment des contrôles du respect des règles relatives au Règlement sur la cybersécurité.

L'article 58, § 4, du Règlement exige que les activités de l'autorité nationale de cybersécurité en matière de délivrance de certificats de cybersécurité européens soient strictement distinctes de ses activités de supervision, et à ce que ces deux activités soient exécutées indépendamment l'une de l'autre.

Lors de l'accomplissement de ses missions de contrôle, le service d'inspection de l'autorité nationale de cybersécurité sera entièrement autonome des autres départements de cette autorité, notamment du service chargé de la délivrance des certificats.

Afin d'assurer cette indépendance fonctionnelle et cette séparation des tâches, le service d'inspection sera doté d'un directeur, de membres du personnel et d'outils propres pour accomplir ses tâches de supervision.

Conformément aux articles 58, § 5, et 59, § 2, du Règlement sur la cybersécurité, le service d'inspection doit, afin d'assurer ses missions de contrôle, disposer des moyens humains et budgétaires suffisants.

Toutefois, ce service d'inspection pourra faire appel à des experts, lesquels sont soumis également au secret professionnel prévu par le paragraphe 4, en fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité.

L'autorité nationale pourrait ainsi faire appel à des experts externes, par exemple, des organismes privés, des autorités de surveillance du marché ou des autorités sectorielles. Ces experts disposent également d'une certaine expertise dans le contrôle des produits, services ou processus. Une mise en œuvre combinée des contrôles entre les autorités compétentes en vertu de différentes législations est de nature à renforcer le travail de surveillance du marché, ce qui est aussi explicitement prévu par le Règlement sur la cybersécurité. Ainsi, l'article 58, § 7, a), du Règlement sur la cybersécurité précise bien que les tâches de supervision de l'autorité nationale de certification de cybersécurité doivent être réalisées en coopération avec les autres autorités compétentes de surveillance du marché.

Cette disposition permet une collaboration entre l'autorité nationale de certification de cybersécurité ou l'autorité visée à l'article 5, § 2 et une autre autorité publique lorsque les deux parties y trouvent un intérêt commun. Les experts de l'autorité publique demeureraient attachés à leur service d'origine et se verraient confier,

koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.

Artikel 58, lid 4, van de Verordening vereist dat de werkzaamheden van de nationale cyberbeveiligingscertificeringsautoriteit met betrekking tot de afgifte van Europese cyberbeveiligingscertificaten strikt gescheiden zijn van haar toezichthoudende werkzaamheden, en dat beide werkzaamheden onafhankelijk van elkaar worden verricht.

De inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit vervult zijn toezichtsopdrachten volledig autonoom van de andere departementen van deze autoriteit, met name van de dienst belast met de afgifte van certificaten.

Om deze functionele onafhankelijkheid en taakverdeling te garanderen, beschikt de inspectiedienst over een eigen directeur en over eigen personeelsleden en middelen om zijn toezichtstaken te vervullen.

Overeenkomstig de artikelen 58, lid 5, en 59, lid 2, van de Cyberbeveiligingsverordening moet de inspectiedienst over voldoende menselijke en budgettaire middelen beschikken om zijn toezichtsopdrachten te vervullen.

Deze inspectiedienst kan echter een beroep doen op experten, die ook onderworpen zijn aan het in paragraaf 4 bedoelde beroepsgeheim, naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling.

Zo kan de nationale autoriteit een beroep doen op externe experten, bijvoorbeeld van privéinstanties, markttoezichtautoriteiten of sectorale overheden. Deze experten beschikken ook over een bepaalde expertise inzake de controle van producten, diensten of processen. De combinatie van controles door de krachtens verschillende wetgevingen bevoegde autoriteiten kan het markttoezicht versterken, wat ook uitdrukkelijk bepaald is in de Cyberbeveiligingsverordening. Zo verduidelijkt artikel 58, lid 7, onder a), van de Cyberbeveiligingsverordening dat de nationale cyberbeveiligingscertificeringsautoriteit haar toezichtstaken moet vervullen in samenwerking met de andere betrokken markttoezichtautoriteiten.

Deze bepaling biedt de mogelijkheid tot samenwerking tussen de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2, en een andere overheid wanneer beide partijen daar belang bij hebben. De experten van de overheid zouden verbonden blijven aan hun dienst van oorsprong en, met het

avec l'accord de cette dernière, des tâches ponctuelles d'assistance pour les services de l'autorité nationale de certification de cybersécurité ou de l'autorité visée à l'article 5, § 2.

Les frais d'experts externes requis par le service d'inspection peuvent être mis à charge des organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens ou les émetteurs de déclarations de conformité de l'Union européenne dès lors que, d'une part, ces derniers sollicitent volontairement une autorisation ou une certification, et d'autre part, ces derniers pourraient en tirer un avantage pécuniaire ou commercial.

Le dernier paragraphe tient les membres du personnel du service d'inspection au secret professionnel. En effet, une absence de garanties suffisantes quant au traitement confidentiel des informations fournies au service d'inspection dans le cadre de sa mission de contrôle risquerait de décourager les entreprises qui voudraient avoir recours à des certifications volontaires de cybersécurité.

Bien entendu, les membres du personnel des autres services de l'autorité nationale de cybersécurité sont tenus au respect de leurs obligations statutaires ou contractuelles en matière de confidentialité.

Art. 14

Cet article prévoit la coopération et l'assistance entre le service d'inspection et les autorités nationales de certification de cybersécurité compétentes d'autres États de l'Union européenne lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificats de cybersécurité européens volontaires ou un émetteur de déclarations de conformité est situé en dehors du territoire belge.

Ces mesures peuvent, par exemple, porter sur des échanges d'informations et sur des demandes de mesures de contrôle.

Art. 15

Les membres du service d'inspection doivent porter une carte de légitimation dont le modèle sera fixé par le Roi.

L'article porte également sur les conflits d'intérêts pouvant concerner les inspecteurs et leur prestation de serment.

akkoord van deze overheid, belast worden met specifieke bijstandstaken voor de diensten van de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2.

De kosten voor externe experten die door de inspectiedienst worden opgeroepen, kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen, aangezien die laatsten enerzijds zelf een toelating of certificering aanvragen en daar anderzijds een financieel of commercieel voordeel uit kunnen halen.

Krachtens de laatste paragraaf zijn de personeelsleden van de inspectiedienst gebonden aan het beroepsgeheim. Het ontbreken van voldoende waarborgen met betrekking tot de vertrouwelijke behandeling van de informatie die aan de inspectiedienst wordt verstrekt in het kader van de toezichtsopdracht van die laatste, kan ondernemingen er immers van weerhouden gebruik te maken van vrijwillige cyberbeveiligingscertificeringen.

Uiteraard moeten de personeelsleden van de andere diensten van de nationale cyberbeveiligingscertificeringsautoriteit hun statutaire of contractuele verplichtingen inzake vertrouwelijkheid nakomen.

Art. 14

Volgens dit artikel is samenwerking en bijstand toegestaan tussen de inspectiedienst en de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van andere landen van de Europese Unie wanneer een conformiteitsbeoordelingsinstantie, een houder van vrijwillige Europese cyberbeveiligingscertificaten of een afgever van EU-conformiteitsverklaringen zich buiten het Belgische grondgebied bevindt.

Deze maatregelen kunnen bijvoorbeeld betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.

Art. 15

De leden van de inspectiedienst moeten een legitimatiekaart bij zich hebben waarvan het model door de Koning wordt bepaald.

Het artikel handelt ook over mogelijke belangenconflicten met betrekking tot inspecteurs en over hun eedaflegging.

Le service d'inspection dispose de larges pouvoirs afin d'effectuer des contrôles approfondis du respect du Règlement sur la cybersécurité et de la présente loi. Étant donné l'étendue des pouvoirs conférés au service d'inspection, l'article 15 précise, en son dixième paragraphe, que les moyens mis en œuvre par les membres assermentés du service d'inspection doivent être appropriés et nécessaires au contrôle du respect du Règlement sur la cybersécurité, de la présente loi et des schémas de certification concernés.

Les membres du service d'inspection peuvent notamment pénétrer sans avertissement préalable dans tous les locaux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens volontaires ou l'émetteur de déclarations de conformité de l'Union européenne.

Les membres du service d'inspection peuvent pénétrer dans les locaux habités moyennant une autorisation préalable d'un juge d'instruction.

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

Par ailleurs, lorsque cela s'avère nécessaire pour leurs missions de contrôle, les membres du service d'inspection devront disposer de l'habilitation de sécurité correspondant au niveau de classification, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, des informations auxquelles ils doivent avoir accès.

Enfin, il est possible, pour les membres assermentés du service d'inspection, d'avoir accès aux informations protégées par le secret professionnel lors de leurs contrôles.

En effet, l'accès aux produits, services ou processus TIC faisant l'objet de la certification dont serait titulaire une personne soumise à l'article 458 du Code pénal pourra être nécessaire afin de mener à bien les missions de supervision du service d'inspection. Les membres assermentés doivent pouvoir, le cas échéant, avoir accès à ces produits, services ou processus TIC.

Néanmoins, étant donné la criticité de ces informations et la protection qu'il convient de lui fournir, la disposition prévoit, de manière claire, que l'accès à ces informations n'est possible pour les membres assermentés, seulement lorsque cet accès est nécessaire à leurs missions de supervision. Par ailleurs, il faut souligner que les membres assermentés ne sont pas des officiers de police judicaire.

De inspectiedienst beschikt over ruime bevoegdheden om grondige controles uit te voeren op de naleving van de Cyberbeveiligingsverordening en deze wet. Gezien de omvang van de bevoegdheden van de inspectiedienst verduidelijkt artikel 15, § 10, dat de middelen die de beëdigde leden van de inspectiedienst gebruiken, passend en noodzakelijk moeten zijn voor het toezicht op de naleving van de Cyberbeveiligingsverordening, van deze wet en van de betrokken certificeringsregelingen.

De leden van de inspectiedienst mogen met name zonder voorafgaande verwittiging alle lokalen betreden die gebruikt worden door de conformiteitsbeoordelingsinstantie, de houder van vrijwillige Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen.

De leden van de inspectiedienst mogen de bewoonde lokalen betreden mits voorafgaande machtiging van een onderzoeksrechter.

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

Bovendien moeten de leden van de inspectiedienst, indien dit nodig is voor hun toezichtsopdrachten, over de veiligheidsmachtiging beschikken die overeenstemt met het classificatieniveau, als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de informatie waar zij toegang toe moeten hebben.

Tot slot kunnen beëdigde leden van de inspectiedienst tijdens hun inspecties toegang krijgen tot informatie die onder het beroepsgeheim valt.

De toegang tot ICT-producten, -diensten of -processen die het voorwerp uitmaken van het certificaat waarvan een persoon die onder artikel 458 van het Strafwetboek valt, houder is, kan immers noodzakelijk zijn om de toezichtsopdrachten van de inspectiedienst uit te voeren. In voorkomend geval moeten de beëdigde leden toegang kunnen krijgen tot deze ICT-producten, -diensten of -processen.

Gelet op het kritieke karakter van deze informatie en de bescherming die ze moet krijgen, verduidelijkt de bepaling niettemin dat de beëdigde leden alleen toegang tot deze informatie kunnen krijgen indien die toegang noodzakelijk is voor hun toezichtsopdrachten. Voorts moet worden beklemtoond dat beëdigde leden geen officieren van gerechtelijke politie zijn. Zij kunnen

Ils ne peuvent faire usage de la contrainte à l'encontre des personnes contrôlées et ne peuvent, dès lors, forcer l'accès aux informations protégées par l'article 458 du Code pénal. De cette manière, la présente disposition s'aligne à ce que prévoit l'article 86 de la loi du 7 décembre 2016 portant organisation de la profession et de la supervision publique des réviseurs d'entreprises.

L'Autorité de protection des données préconise une disposition reprenant des garanties similaires à ce que prévoient les articles 56*bis* et 90*octies* du Code d'instruction criminelle. À défaut, le projet de loi doit préciser qu'aucune collecte de ces informations protégées n'est possible.

Étant donné que les pouvoirs du service d'inspection sont bien plus limités que ce que prévoit le Code d'instruction criminelle aux article 56*bis* et 90*octies*, il a été décidé de ne pas implémenter les garanties demandées par l'Autorité de protection des données dans son avis.

Art. 16

Le rapport d'inspection est transmis 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.

Afin de préserver le droit des personnes concernées, le paragraphe 2 dispose que les rapports ne peuvent contenir de données à caractère personnel des clients (ou des données à caractère personnel traitées par ces derniers) des titulaires de certificats de cybersécurité ou des émetteurs de déclarations de conformité contrôlés.

Ce rapport pourra être communiqué à l'autorité nationale d'accréditation ou à l'Institut belge des services postaux et des télécommunications, à leur demande, dans le cadre des missions de contrôle des activités des organismes d'évaluation de la conformité, 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, § 7, c), et 60, § 1er et § 4, du Règlement sur la cybersécurité ou des compétences en matière de cybersécurité prévues aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques.

Le deuxième alinéa du paragraphe 3 permet de déroger à l'obligation de formaliser un transfert de données à caractère personnel par un protocole, prévue à

geen gebruik maken van dwang jegens gecontroleerde personen en kunnen bijgevolg geen toegang afdwingen tot informatie die door artikel 458 van het Strafwetboek beschermd is. Op die manier sluit deze bepaling aan bij artikel 86 van de wet van 7 december 2016 tot organisatie van het beroep van en het publiek toezicht op de bedrijfsrevisoren.

De Gegevensbeschermingsautoriteit pleit voor een bepaling met soortgelijke waarborgen als in artikel 56*bis* en 90*octies* van het Wetboek van strafvordering. Zo niet moet het wetsontwerp erop wijzen dat deze beschermde informatie niet mag worden verzameld.

Aangezien de bevoegdheden van de inspectiedienst veel beperkter zijn dan wat in artikel 56*bis* en 90*octies* van het Wetboek van strafvordering is bepaald, werd beslist om de door de Gegevensbeschermingsautoriteit in haar advies gevraagde waarborgen niet op te nemen.

Art. 16

Het inspectieverslag wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van Europese cyberbeveiligingscertificaten of afgever van EU-conformiteitsverklaringen.

Om het recht van de betrokkenen te vrijwaren, bepaalt paragraaf 2 dat de verslagen geen persoonsgegevens mogen bevatten van klanten (of persoonsgegevens die laatstgenoemden verwerken) van gecontroleerde houders van cyberbeveiligingscertificaten of afgevers van conformiteitsverklaringen.

Dit verslag kan worden bezorgd aan de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie, op verzoek van laatstgenoemden, in het kader van de opdrachten inzake het toezicht op de activiteiten van conformiteitsbeoordelingsinstanties als 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, lid 1 en lid 4, van de Cyberbeveiligingsverordening, of van de bevoegdheden inzake cyberbeveiliging bedoeld in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Het tweede lid van paragraaf 3 laat toe af te wijken van de verplichting om een doorgifte van persoonsgegevens te formaliseren aan de hand van een protocol,

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, pour autant que les conditions énoncées aux 1° à 4° soient respectées. Ces conditions ont pour objectif de préciser explicitement, comme le préconise l'Autorité de protection des données à la page 16 de sa Recommandation n° 02/2020 du 31 janvier 2020 relative à la portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral, "qui (destinataire) se voit transmettre quoi (catégories précises des données communiquées), quand et pourquoi (finalités et modalités de la communication)".

Le paragraphe 4 prévoit que lorsque des contrôles sont effectués auprès d'une infrastructure critique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien ou auprès d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi NIS, le rapport prévu au paragraphe 1er est automatiquement transmis à l'autorité sectorielle et au service d'inspection compétents. En effet, d'une manière similaire à ce que prévoit l'article 6, § 3, les compétences en matière de cybersécurité, décrites au commentaire de l'article 6, dont sont pourvus les autorités sectorielles et les services d'inspection précités, justifient un tel transfert auprès de ceux-ci.

D'une manière similaire au deuxième alinéa du paragraphe 3, le troisième alinéa du paragraphe 4 permet, selon des conditions identiques, de déroger 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. Cette disposition est reprise au sein de ce paragraphe car, comme l'a précisé l'Autorité de protection des données dans son avis n° 08/2022 du 21 janvier 2022, au considérant 84, le flux de données à caractère personnel doit être encadré au niveau des dispositions qui, elles-mêmes, encadrent les communications de données.

Lorsqu'un rapport d'inspection contient des données à caractère personnel, le chapitre 8 s'applique.

Les échanges d'informations prévus aux paragraphes 3 et 4 de cet article sont prévus car, même lorsque les contrôles effectués ne mènent pas à une décision de retrait, les rapports peuvent se révéler importants pour les autorités citées. Dès lors, la publicité des décisions de retrait ne constitue pas un échange d'informations suffisant.

bedoeld in artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, voor zover de in 1° tot 4° vermelde voorwaarden vervuld zijn. Deze voorwaarden hebben tot doel om, zoals de Gegevensbeschermingsautoriteit bepleit op bladzijde 16 van haar Aanbeveling nr. 02/2020 van 31 januari 2020 betreffende de draagwijdte van de verplichting om een protocol te sluiten om de mededelingen van persoonsgegevens door de federale publieke sector te formaliseren, uitdrukkelijk te bepalen "aan wie (ontvanger) wat wordt [sic] (precieze categorieën van meegedeelde gegevens), wanneer en waarom (doeleinden en modaliteiten van de mededeling) wordt doorgegeven".

Paragraaf 4 bepaalt dat indien controles worden uitgevoerd bij een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of in het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer of bij een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in de NIS-wet, het verslag bedoeld in paragraaf 1 automatisch aan de bevoegde sectorale overheid en inspectiedienst wordt bezorgd. Op soortgelijke wijze als wat in artikel 6, § 3, is bepaald, is deze overdracht immers gerechtvaardigd in het licht van de in de commentaar bij artikel 6 beschreven bevoegdheden inzake cyberbeveiliging van voornoemde sectorale overheden en inspectiediensten.

Op soortgelijke wijze als in het tweede lid van paragraaf 3 laat het derde lid van paragraaf 4 toe om, onder dezelfde voorwaarden, af te wijken van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Deze bepaling is in deze paragraaf opgenomen omdat, zoals de Gegevensbeschermingsautoriteit in overweging 84 van haar advies nr. 08/2022 van 21 januari 2022 heeft verklaard, een kader moet worden geboden voor de stroom van persoonsgegevens op het niveau van de bepalingen die zelf een kader bieden voor de mededelingen van gegevens.

Indien een inspectieverslag persoonsgegevens bevat, is hoofdstuk 8 van toepassing.

De in paragraaf 3 en 4 van dit artikel bedoelde informatie-uitwisseling is voorzien omdat, zelfs wanneer de uitgevoerde controles niet tot een intrekkingsbeslissing leiden, de verslagen van belang kunnen zijn voor de vermelde overheden. Bijgevolg volstaat de openbaarmaking van intrekkingsbeslissingen niet als informatie-uitwisseling.

Art. 17

Cet article porte sur les procès-verbaux rédigés par les membres assermentés du service d'inspection, au travers desquels ils constatent les manquements aux obligations découlant du projet de loi ou du Règlement sur la cybersécurité.

Le procès-verbal, établi suite à un contrôle, peut, à la demande de l'autorité nationale d'accréditation ou de l'Institut belge des services postaux et des télécommunications, pour autant que cette demande soit faite, soit dans le cadre des compétences légales 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, § 7, c), et 60, § 1er et § 4, du Règlement sur la cybersécurité, soit dans le cadre des compétences prévues aux articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, lui être transmis par l'autorité nationale de certification de cybersécurité ou l'autorité à laquelle le Roi aura attribué certaines missions de contrôle conformément à l'article 5, § 2.

Le deuxième alinéa du paragraphe 2 permet de déroger à l'obligation de formaliser un transfert de données à caractère personnel par un protocole, prévue 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, pour autant que les conditions énoncées aux 1° à 4° soient respectées. Ces conditions ont pour objectif de préciser explicitement, comme le préconise l'Autorité de protection des données à la page 16 de sa Recommandation n° 02/2020 du 31 janvier 2020 relative à la portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral, "qui (destinataire) se voit transmettre quoi (catégories précises de données communiquées), quand et pourquoi (finalités et modalités de la communication)". Cette disposition, identique à l'alinéa 2 du paragraphe 3 de l'article 16, est reprise ici car, comme l'a précisé l'Autorité de protection des données dans son avis n° 08/2022 du 21 janvier 2022, au considérant 84, le flux de données à caractère personnel doit être encadré au niveau des dispositions qui, elles-mêmes, encadrent les communications de données.

Art. 17

Dit artikel heeft betrekking op de processen-verbaal die de beëdigde leden van de inspectiedienst opstellen voor de vaststelling van inbreuken op de verplichtingen die voortvloeien uit het wetsontwerp of de Cyberbeveiligingsverordening.

Het na een controle opgestelde proces-verbaal kan door de nationale cyberbeveiligingscertificeringsautoriteit of de overheid waaraan de Koning bepaalde toezichtsopdrachten heeft toegekend overeenkomstig artikel 5, § 2, worden bezorgd aan de nationale accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie, op verzoek van laatstgenoemden en voor zover dit verzoek kadert hetzij in de wettelijke bevoegdheden 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, lid 1 en lid 4, van de Cyberbeveiligingsverordening, hetzij in de bevoegdheden bedoeld in de artikelen 107/2 tot 107/5 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Het tweede lid van paragraaf 2 laat toe af te wijken van de verplichting om een doorgifte van persoonsgegevens te formaliseren aan de hand van een protocol, bedoeld in artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, voor zover de in 1° tot 4° vermelde voorwaarden vervuld zijn. Deze voorwaarden hebben tot doel om, zoals de Gegevensbeschermingsautoriteit bepleit op bladzijde 16 van haar Aanbeveling nr. 02/2020 van 31 januari 2020 betreffende de draagwijdte van de verplichting om een protocol te sluiten om de mededelingen van persoonsgegevens door de federale publieke sector te formaliseren, uitdrukkelijk te bepalen "aan wie (ontvanger) wat wordt [sic] (precieze categorieën van meegedeelde gegevens), wanneer en waarom (doeleinden en modaliteiten van de mededeling) wordt doorgegeven". Deze bepaling, die overeenstemt met het tweede lid van paragraaf 3 van artikel 16, is hier opgenomen omdat, zoals de Gegevensbeschermingsautoriteit in overweging 84 van haar advies nr. 08/2022 van 21 januari 2022 heeft verklaard, een kader moet worden geboden voor de stroom van persoonsgegevens op het niveau van de bepalingen die zelf een kader bieden voor de mededelingen van gegevens.

Le paragraphe 3 prévoit que l'autorité nationale de certification de cybersécurité ou l'autorité visée à l'article 5, § 2 transmet automatiquement à l'autorité sectorielle ou au service d'inspection concerné les informations relatives à un contrôle, en ce compris le procès-verbal, effectué auprès d'une infrastructure critique, d'un opérateur de services essentiels ou d'un fournisseur de service numérique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien ou de la loi NIS. En effet, d'une manière similaire à ce que prévoient les articles 6, § 3, et 16, § 3, les compétences en matière de cybersécurité, décrites au commentaire de l'article 6, dont sont pourvus les autorités sectorielles et les services d'inspection précités, justifient un tel transfert auprès de ceux-ci.

D'une manière similaire au deuxième alinéa du paragraphe 2, le troisième alinéa du paragraphe 3 permet, selon des conditions identiques, de déroger 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. Cette disposition est reprise au sein de ce paragraphe car, comme l'a précisé l'Autorité de protection des données dans son avis n° 08/2022 du 21 janvier 2022, au considérant 84, le flux de données à caractère personnel doit être encadré au niveau des dispositions qui, elles-mêmes, encadrent les communications de données.

Lorsque les informations concernées par cette disposition ou un procès-verbal contient des données à caractère personnel, le chapitre 8 s'applique.

Les échanges d'informations prévues aux paragraphes 2 et 3 de cet article sont prévus car, même lorsque les contrôles effectués ne mènent pas à une décision de retrait, les procès-verbaux peuvent se révéler importants pour les autorités citées. Dès lors, la publicité des décisions de retrait ne constitue pas un échange d'informations suffisant.

Art. 18

Cette disposition porte sur la collaboration entre les personnes visées par une inspection et le service d'inspection ou les experts.

Le Roi peut déterminer des rétributions relatives à la délivrance et aux prestations d'inspections. Il s'agit, en effet, de prévoir la possibilité, le cas échéant, de couvrir les frais assumés par le service d'inspection de l'autorité nationale de certification de cybersécurité

Paragraaf 3 bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2, de betrokken sectorale overheid of inspectiedienst automatisch de informatie, met inbegrip van het proces-verbaal, bezorgt die betrekking heeft op een controle bij een kritieke infrastructuur, aanbieder van essentiële diensten of digitaledienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer of de NIS-wet. Op soortgelijke wijze als wat bepaald is in de artikelen 6, § 3, en 16, § 3, is deze overdracht immers gerechtvaardigd in het licht van de in de commentaar bij artikel 6 beschreven bevoegdheden inzake cyberbeveiliging van voornoemde sectorale overheden en inspectiediensten.

Op soortgelijke wijze als in het tweede lid van paragraaf 2 laat het derde lid van paragraaf 3 toe om, onder dezelfde voorwaarden, af te wijken van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Deze bepaling is in deze paragraaf opgenomen omdat, zoals de Gegevensbeschermingsautoriteit in overweging 84 van haar advies nr. 08/2022 van 21 januari 2022 heeft verklaard, een kader moet worden geboden voor de stroom van persoonsgegevens op het niveau van de bepalingen die zelf een kader bieden voor de mededelingen van gegevens.

Indien de informatie waarop deze bepaling betrekking heeft of een proces-verbaal persoonsgegevens bevat, is hoofdstuk 8 van toepassing.

De in paragraaf 2 en 3 van dit artikel bedoelde informatie-uitwisseling is voorzien omdat, zelfs wanneer de uitgevoerde controles niet tot een intrekkingsbeslissing leiden, de processen-verbaal van belang kunnen zijn voor de vermelde overheden. Bijgevolg volstaat de openbaarmaking van intrekkingsbeslissingen niet als informatie-uitwisseling.

Art. 18

Deze bepaling heeft betrekking op de samenwerking tussen de personen die aan een inspectie worden onderworpen en de inspectiedienst of de experten.

De Koning kan retributies bepalen voor de afgifte en de inspectieprestaties. Het is immers de bedoeling te voorzien in de mogelijkheid om, in voorkomend geval, de kosten te dekken die de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit of van de

ou de l'autorité visée à l'article 5, § 2 en raison des certifications européennes volontaires accordées en Belgique (frais d'expert, frais de personnel, frais administratifs, etc.).

CHAPITRE 6

Sanctions

Section 1re

Procédure

Art. 19

L'article prévoit une mise en demeure préalable en cas de manquement constaté par le service d'inspection.

Préalablement à cette mise en demeure, le contrevenant est informé de l'intention du service d'inspection de le mettre en demeure.

Art. 20

Cette disposition porte sur le constat du non-respect des obligations découlant de la loi ou du Règlement sur la cybersécurité. Ainsi, même si le contrevenant se conforme à la mise en demeure adressée par le service d'inspection, cela n'empêche pas la rédaction d'un procès-verbal et l'imposition d'une sanction à son encontre.

Les procès-verbaux font foi jusqu'à preuve du contraire.

Section 2

Retrait d'un certificat

Art. 21

En cas de non-respect du Règlement sur la cybersécurité ou d'un schéma européen de certification de cybersécurité, l'autorité nationale de certification de cybersécurité peut retirer un certificat de cybersécurité.

L'article 58, § 8, e), du Règlement sur la cybersécurité précise bien que l'autorité de certification de cybersécurité peut retirer les certificats de cybersécurité européens délivrés lorsque de tels certificats ne respectent pas ledit Règlement ou un schéma européen de certification de cybersécurité.

overheid bedoeld in artikel 5, § 2, maakt in het kader van vrijwillige Europese certificeringen die in België worden toegekend (kosten voor experten, personeelskosten, administratieve kosten, enz.).

HOOFDSTUK 6

Sancties

Afdeling 1

Procedure

Art. 19

Het artikel voorziet in een voorafgaande ingebrekestelling ingeval de inspectiedienst een inbreuk vaststelt.

Vóór deze ingebrekestelling deelt de inspectiedienst de overtreder mee dat hij van plan is hem in gebreke te stellen.

Art. 20

Deze bepaling heeft betrekking op de vaststelling dat de verplichtingen van de wet of de Cyberbeveiligingsverordening niet zijn nagekomen. Zelfs als de overtreder gevolg geeft aan de ingebrekestelling van de inspectiedienst, kan een proces-verbaal worden opgesteld en een sanctie worden opgelegd.

De processen-verbaal hebben bewijskracht tot het tegendeel is bewezen.

Afdeling 2

Intrekking van een certificaat

Art. 21

Ingeval de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet wordt nageleefd, kan de nationale cyberbeveiligingscertificeringsautoriteit een cyberbeveiligingscertificaat intrekken.

Volgens artikel 58, lid 8, onder e), van de Cyberbeveiligingsverordening kan de cyberbeveiligingscertificeringsautoriteit afgegeven Europese cyberbeveiligingscertificaten intrekken als ze niet voldoen aan deze verordening of aan een Europese cyberbeveiligingscertificeringsregeling.

Dans son avis n° 08/2022 du 21 janvier 2022, l'Autorité de protection des données demandait à ce que la présente loi impose, à l'autorité nationale de certification de cybersécurité, une obligation d'information relative aux retraits de certificats, au travers d'un site web et d'un service d'information (push) qui notifie à tous les acteurs concernés tout retrait de certification. Cette remarque (n° 2) de l'Autorité de protection des données n'a pas été suivie.

En effet, la présente loi ne devrait pas imposer d'obligation d'information car, selon l'article 54, § 1er, p) et s), du Règlement sur la Cybersécurité, tout schéma européen de certification de cybersécurité comprend, entre autres, au moins "le contenu et le format des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne à délivrer" ainsi que "la politique de divulgation concernant les certificats de cybersécurité européens délivrés, modifiés ou retirés dans le cadre du schéma". Les schémas européens de certification de cybersécurité préciseront eux-mêmes les modalités de publicité relatives à la délivrance, la modification ou le retrait des certificats concernés.

De plus, comme le prévoit l'article 50, § 1er, l'ENISA tient à jour un site internet dédié qui fournit, entre autres, des informations relatives aux certificats de cybersécurité européens qui ont été retirés ou ont expiré et aux déclarations de conformité de l'Union européenne.

Il ressort de ces articles que la publicité relative aux certificats de cybersécurité européens est déjà organisée par le Règlement sur la cybersécurité.

Par ailleurs, contrairement à ce qu'avance l'Autorité de protection des données, la publicité suggérée par cette dernière au considérant 15 de son avis n° 08/2022 du 21 janvier 2022 entraîne également un traitement de données à caractère personnel lorsque le titulaire du certificat faisant l'objet du retrait est une personne physique.

Section 3

Limitation, suspension ou retrait d'une autorisation ou d'une délégation

Art. 22

Les autorisations accordées aux organismes d'évaluation de la conformité en vertu de l'article 60, § 3, du Règlement sur la cybersécurité ainsi que les délégations effectuées en vertu des articles 10 et 11 peuvent être limitées, suspendues ou retirées par l'autorité nationale de certification de cybersécurité.

In haar advies nr. 08/2022 van 21 januari 2022 heeft de Gegevensbeschermingsautoriteit gevraagd om in deze wet een informatieplicht inzake intrekkingen van certificaten op te leggen aan de nationale cyberbeveiligingscertificeringsautoriteit, via een website en een informatiedienst (push) die alle betrokken actoren op de hoogte brengt van elke certificeringsintrekking. Aan deze opmerking (nr. 2) van de Gegevensbeschermingsautoriteit is geen gevolg gegeven.

Deze wet moet immers geen informatieplicht opleggen omdat, volgens artikel 54, lid 1, onder p) en s), van de Cyberbeveiligingsverordening, elke Europese cyberbeveiligingscertificeringsregeling onder meer ten minste "de inhoud en vorm van de af te geven Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen", alsook "het openbaarmakingsbeleid inzake uit hoofde van de regeling afgegeven, gewijzigde en ingetrokken Europees [sic] cyberbeveiligingscertificaten" omvat. De Europese cyberbeveiligingscertificeringsregelingen zullen zelf de bekendmakingsmodaliteiten betreffende de afgifte, wijziging of intrekking van de betrokken certificaten preciseren.

Zoals bepaald in artikel 50, lid 1, beheert Enisa bovendien een specifieke website met onder meer informatie over ingetrokken of verstreken Europese cyberbeveiligingscertificaten en over EU-conformiteitsverklaringen.

Uit deze artikelen blijkt dat de bekendmaking van Europese cyberbeveiligingscertificaten al wordt geregeld door de Cyberbeveiligingsverordening.

In tegenstelling tot wat de Gegevensbeschermingsautoriteit verklaart, gaat de openbaarmaking die laatstgenoemde in overweging 15 van haar advies nr. 08/2022 van 21 januari 2022 voorstelt, overigens ook gepaard met een verwerking van persoonsgegevens wanneer de houder van het certificaat dat wordt ingetrokken, een natuurlijk persoon is.

Afdeling 3

Beperken, opschorten of intrekken van een toelating of een delegatie

Art. 22

De nationale cyberbeveiligingscertificeringsautoriteit kan toelatingen die krachtens artikel 60, § 3, van de Cyberbeveiligingsverordening aan conformiteitsbeoordelingsinstanties zijn verleend en delegaties die krachtens de artikelen 10 en 11 zijn verleend, beperken, opschorten of intrekken.

Section 4

Amendes administratives

Cette section précise le principe et les montants des amendes administratives et souligne les possibilités de recours à cet égard.

L'article 65 du Règlement sur la cybersécurité prévoit que les violations des règles prévues par le Règlement et par les schémas européens de certification de cybersécurité doivent faire l'objet de sanctions. Comme le précise cet article, les sanctions doivent être effectives, proportionnées et dissuasives.

Si le retrait de la certification constitue une forme de sanction, il est nécessaire que l'autorité de certification de cybersécurité dispose également d'une gamme plus étendue et plus dissuasive d'instruments de sanction que le seul retrait de la certification.

Bien entendu, si les sanctions doivent être dissuasives, elles doivent également être proportionnées. L'amende doit être proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de fait.

Chaque État membre de l'Union européenne doit, d'ailleurs, informer la Commission du régime de sanction et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

Cette section prévoit une compétence de pleine juridiction pour la Cour des marchés, en ce qui concerne les recours des décisions de sanctions de l'autorité nationale de certification de cybersécurité ou de l'autorité visée à l'article 5, § 2, prises en vertu du chapitre 6.

Cette Cour a été choisie car elle constitue déjà une juridiction compétente pour des recours similaires prévus par d'autres législations, telles que la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, 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 (loi NIS) ou encore la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. De plus, il s'agit d'une juridiction spécialisée qui sera à même de fournir l'expertise requise.

Afdeling 4

Administratieve geldboetes

Deze afdeling verduidelijkt het principe en de bedragen van de administratieve geldboetes en wijst op de beroepsmogelijkheden in dit verband.

Volgens artikel 65 van de Cyberbeveiligingsverordening moeten inbreuken op de regels van de Verordening en van de Europese cyberbeveiligingscertificeringsregelingen aanleiding geven tot sancties. Zoals verduidelijkt in dit artikel moeten de sancties doeltreffend, evenredig en afschrikkend zijn.

Hoewel de intrekking van de certificering een vorm van sanctie is, moet de cyberbeveiligingscertificeringsautoriteit ook over een bredere en meer afschrikkende waaier aan sanctie-instrumenten beschikken dan de loutere intrekking van de certificering.

De sancties moeten afschrikkend zijn, maar uiteraard ook evenredig. De geldboete moet in verhouding staan tot de ernst, duur, gebruikte middelen, veroorzaakte schade en feitelijke omstandigheden.

Iedere lidstaat van de Europese Unie moet de Commissie overigens in kennis stellen van de sanctieregeling en de genomen maatregelen alsook van alle eventuele latere wijzigingen van deze regeling of maatregelen.

Deze afdeling voorziet in volle rechtsmacht voor het Marktenhof wat betreft beroepsprocedures tegen sanctiebeslissingen die de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2, krachtens hoofdstuk 6 heeft genomen.

Dit Hof werd als rechtscollege gekozen omdat het al bevoegd is voor soortgelijke beroepsprocedures waarin andere wetgevingen voorzien, zoals de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, 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 (NIS-wet) of nog de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Bovendien is het een gespecialiseerd rechtscollege dat de vereiste expertise kan inbrengen.

CHAPITRE 7

Réclamations

Section 1re

Saisine de l'autorité nationale de certification de cybersécurité

Cette section prévoit les modalités de saisine de l'autorité nationale de certification de cybersécurité pour statuer sur les réclamations en rapport avec un certificat de cybersécurité européen, un refus de délivrance d'un certificat ou une déclaration de conformité de l'Union européenne.

Conformément à l'article 63, § 1er, du Règlement, les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité agissant conformément à l'article 56, paragraphe 6, auprès de l'autorité nationale de certification de cybersécurité concernée.

L'article 58, § 7, f), du Règlement confirme que l'autorité nationale de certification de cybersécurité est compétente pour traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par elle, en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 56, paragraphe 6 ainsi qu'en rapport avec les déclarations de conformité de l'Union européenne.

Il ressort du Règlement qu'en principe, les personnes physiques ou morales adressent leurs réclamations à l'entité concernée par la délivrance du certificat de cybersécurité européen en question, c'est-à-dire l'organisme d'évaluation de la conformité, l'autorité nationale de certification de cybersécurité ou l'organisme publique chargé de la délivrance d'un certificat de cybersécurité européen, en fonction du schéma européen de certification de cybersécurité.

L'autorité nationale de certification de cybersécurité n'est compétente, pour connaître des réclamations des personnes physiques ou morales en rapport avec un certificat de cybersécurité européen, que lorsque ce dernier est délivré par elle, dans le cadre d'un certificat de cybersécurité européen de niveau "élevé" dont la délivrance a été délégué à un organisme d'évaluation de la conformité ou dans le cadre d'une déclaration de conformité de l'Union européenne.

HOOFDSTUK 7

Klachten

Afdeling 1

Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit

Deze afdeling bepaalt de nadere regels om klachten over een Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of een EU-conformiteitsverklaring aanhangig te maken bij de nationale cyberbeveiligingscertificeringsautoriteit.

Overeenkomstig artikel 63, lid 1, van de Verordening hebben natuurlijke en rechtspersonen het recht een klacht in te dienen bij de afgever van een Europees cyberbeveiligingscertificaat of, wanneer de klacht verband houdt met een Europees cyberbeveiligingscertificaat dat is afgegeven door een conformiteitsbeoordelingsinstantie handelend overeenkomstig artikel 56, lid 6, bij de bevoegde nationale cyberbeveiligingscertificeringsautoriteit.

Artikel 58, lid 7, onder f), van de Verordening bevestigt dat de nationale cyberbeveiligingscertificeringsautoriteit bevoegd is voor de behandeling van klachten van natuurlijke of rechtspersonen over door haar of overeenkomstig artikel 56, lid 6, door conformiteitsbeoordelingsinstanties afgegeven Europese cyberbeveiligingscertificaten, en over EU-conformiteitsverklaringen.

Uit de Verordening blijkt dat natuurlijke en rechtspersonen hun klachten in principe richten aan de entiteit die bevoegd is voor de afgifte van het Europees cyberbeveiligingscertificaat in kwestie, d.w.z. de conformiteitsbeoordelingsinstantie, de nationale cyberbeveiligingscertificeringsautoriteit of de overheidsinstelling belast met de afgifte van een Europees cyberbeveiligingscertificaat, naargelang de Europese cyberbeveiligingscertificeringsregeling.

De nationale cyberbeveiligingscertificeringsautoriteit is enkel bevoegd om kennis te nemen van klachten van natuurlijke of rechtspersonen over een Europees cyberbeveiligingscertificaat wanneer dat certificaat door haar is afgegeven, in het kader van een Europees cyberbeveiligingscertificaat voor niveau "hoog" waarvan de afgifte aan een conformiteitsbeoordelingsinstantie is gedelegeerd of in het kader van een EU-conformiteitsverklaring.

Conformément à l'article 21, l'autorité nationale de certification de cybersécurité peut notamment retirer un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité. L'autorité nationale de certification de cybersécurité peut également limiter, suspendre ou retirer les autorisations et délégations qu'elle a accordées aux organismes d'évaluation de la conformité, comme le prévoit l'article 22.

Section 2

Recours

Art. 35

Comme le prévoit l'article 64 du Règlement sur la cybersécurité, les personnes physiques ou morales disposent d'un droit de recours juridictionnel effectif en ce qui concerne les décisions prises par l'autorité nationale de certification de cybersécurité ou par l'organisme d'évaluation de la conformité accrédité, en ce qui concerne la délivrance non justifiée, la non-délivrance ou la reconnaissance d'un certificat de cybersécurité européen détenu par ces personnes physiques ou morales, ainsi qu'en l'absence de réaction suite à une réclamation.

À cette fin, cet article instaure une compétence de pleine juridiction pour la Cour des marchés.

Cette Cour a été choisie car elle constitue déjà une juridiction compétente pour des recours similaires prévus par d'autres législations, telles que la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, 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 (loi NIS) ou encore la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. De plus, il s'agit d'une juridictions spécialisée qui sera à même de fournir l'expertise requise.

CHAPITRE 8

Traitement des données à caractère personnel

Ce chapitre insère des dispositions relatives aux données à caractère personnel concernées par le projet de loi ainsi qu'à leur traitement.

Bien que certaines dispositions fassent directement référence à ce chapitre, ce dernier a vocation à s'appliquer

Overeenkomstig artikel 21 kan de nationale cyberbeveiligingscertificeringsautoriteit een cyberbeveiligingscertificaat met name intrekken als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft. Zoals bepaald in artikel 22 kan de nationale cyberbeveiligingscertificeringsautoriteit ook toelatingen en delegaties die ze aan conformiteitsbeoordelingsinstanties heeft verleend, beperken, opschorten of intrekken.

Afdeling 2

Beroepen

Art. 35

Volgens artikel 64 van de Cyberbeveiligingsverordening hebben natuurlijke en rechtspersonen recht op een doeltreffende voorziening in rechte met betrekking tot besluiten van de nationale cyberbeveiligingscertificeringsautoriteit of de geaccrediteerde conformiteitsbeoordelingsinstantie betreffende de onjuiste afgifte, het nalaten van afgifte of de erkenning van een Europees cyberbeveiligingscertificaat dat door die natuurlijke of rechtspersonen wordt gehouden, en met betrekking tot het verzuim om gevolg te geven aan een klacht.

Daartoe voorziet dit artikel in volle rechtsmacht voor het Marktenhof.

Dit Hof werd als rechtscollege gekozen omdat het al bevoegd is voor soortgelijke beroepsprocedures waarin andere wetgevingen voorzien, zoals de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, 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 (NIS-wet) of nog de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Bovendien is het een gespecialiseerd rechtscollege dat de vereiste expertise kan inbrengen.

HOOFDSTUK 8

Verwerking van persoonsgegevens

Dit hoofdstuk voegt bepalingen in over de persoonsgegevens waarop het wetsontwerp betrekking heeft en over de verwerking ervan.

Hoewel sommige bepalingen rechtstreeks naar dit hoofdstuk verwijzen, is dit van toepassing op iedere

à tout traitement de données à caractère personnel effectué sur base de ce projet de loi.

Section 1re

Principes relatifs au traitement, base légale et finalités

Art. 36

Le paragraphe premier de cette disposition énumère les finalités de traitement. Il s'agit de l'obligation de délivrance de certificats de cybersécurité européens, des tâches de supervision dévolues au service d'inspection et des tâches de sanction, de la participation au GECC, de la coopération avec les autorités sectorielles et les services d'inspection compétents, visés 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 NIS ou aux articles 2, 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, dans le cadre de leurs missions touchant à la cybersécurité ainsi que de la coopération avec les autres autorités publiques disposant de compétences en matière de cybersécurité.

L'autorité nationale de certification de cybersécurité ou, le cas échéant, les autorités désignées par le Roi pour accomplir certaines missions en matière de contrôle et de sanction sont chacune responsable pour les traitements de données à caractère personnel qu'elles effectuent dans le cadre de l'exécution de la présente loi ou du Règlement sur la Cybersécurité.

Le paragraphe 3 énumère les catégories de données à caractère personnel pouvant être traitées pour chaque finalité énoncée au premier paragraphe.

En ce qui concerne les données à caractère personnel devant être traitées pour la finalité de supervision visée au paragraphe 1er, 2°, la disposition n'énumère pas de catégories de données à caractère personnel à proprement parler. Elle précise que, dans le cadre de cette finalité, toute donnée à caractère personnel nécessaire à son accomplissement peut être traitée.

En effet, comme le reconnaît l'Autorité de protection des données, il n'est pas envisageable de les déterminer autrement que de manière fonctionnelle, en précisant qu'il s'agit des données nécessaires à l'exercice des missions de contrôle et de sanction visées aux chapitres 5 et 6 du projet.

verwerking van persoonsgegevens die op basis van dit wetsontwerp wordt uitgevoerd.

Afdeling 1

Beginselen inzake verwerking, wettelijke basis en doeleinden

Art. 36

De eerste paragraaf van deze bepaling somt de verwerkingsdoeleinden op. Het betreft de verplichting om Europese cyberbeveiligingscertificaten af te geven, de toezichtstaken van de inspectiedienst en de sanctietaken, de deelname aan de EGC, de samenwerking met de bevoegde sectorale overheden en inspectiediensten 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 NIS-wet of in de artikelen 2, 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, in het kader van hun opdrachten inzake cyberbeveiliging en van de samenwerking met andere overheden bevoegd voor cyberbeveiliging.

De nationale cyberbeveiligingscertificeringsautoriteit of, in voorkomend geval, de overheden die voor bepaalde toezichts- en sanctieopdrachten door de Koning zijn aangewezen, zijn elk verantwoordelijk voor de verwerkingen van persoonsgegevens die ze verrichten in het kader van de uitvoering van deze wet of van de Cyberbeveiligingsverordening.

Paragraaf 3 somt de categorieën van persoonsgegevens op die voor elk van de in de eerste paragraaf vermelde doeleinden mogen worden verwerkt.

Wat betreft de persoonsgegevens die moeten worden verwerkt met het oog op het in paragraaf 1, 2°, bedoelde toezicht, somt de bepaling geen categorieën van persoonsgegevens als dusdanig op. Ze vermeldt dat, in het kader van dit doeleinde, alle persoonsgegevens mogen worden verwerkt die voor de verwezenlijking ervan noodzakelijk zijn.

Zoals de Gegevensbeschermingsautoriteit erkent, is het immers niet mogelijk deze anders dan op functionele wijze vast te stellen, door te specificeren dat het gaat om gegevens die noodzakelijk zijn voor de uitoefening van de in hoofdstukken 5 en 6 van het ontwerp bedoelde toezichts- en sanctieopdrachten.

Afin de garantir la proportionnalité des traitements réalisés dans le cadre de cette finalité, la disposition précise que, chaque fois que possible, les données à caractère personnel des clients (ou des données à caractère personnel traitées par ces derniers) des titulaires de certificats de cybersécurité ou des émetteurs de déclarations de conformité contrôlés doivent être pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le RGPD.

Par ailleurs, le quatrième paragraphe prévoit que les échanges entre autorités publiques prévus par la présente loi ne peuvent porter sur des données à caractère personnel des clients (ou des données à caractère personnel traitées par ces derniers) des titulaires de certificats de cybersécurité ou des émetteurs de déclarations de conformité contrôlés.

Le dernier paragraphe énumère, quant à lui, les catégories de personnes concernées par les traitements de données à caractère personnel effectués dans le cadre de l'exécution du Règlement sur la cybersécurité ou de la présente loi.

Art. 37

Cette disposition met en œuvre l'article 23 du Règlement UE 2016/679 (RGPD). Afin d'assurer la sécurité publique et la protection des consommateurs, et dans le cadre des finalités de supervision et de traitement des réclamations visées à l'article 36, § 1er, 2°, les droits des personnes concernées visés aux articles 12 à 16, 18 et 19 du Règlement UE 2016/679 (RGPD) ne sont pas applicables dans les limites prévues par l'article.

L'Autorité de protection des données indique, dans son avis, qu'il n'y a pas lieu de déroger à l'article 12 du RGPD car il ne s'agit pas d'un droit des personnes concernées. Néanmoins, l'article 23, § 1er, du RGPD permet bien de déroger à cet article. La dérogation est donc maintenue.

L'exemption ne vaut que pour les traitements effectués dans le cadre de la finalité de supervision prévue à l'article 36, § 1er, 2°, dans la mesure où l'exercice des droits consacrés par les articles faisant l'objet de la dérogation nuirait aux besoins du contrôle ou des actes préparatoires à celui-ci. Seules l'autorité nationale de certification de cybersécurité ou les autorités désignées par le Roi pour accomplir certaines tâches en matière de contrôle et de sanctions peuvent, lorsqu'elles agissent en tant que responsables de traitement, bénéficier de cette exemption.

Om de evenredigheid van de in het kader van dit doeleinde uitgevoerde verwerkingen te waarborgen, verduidelijkt de bepaling dat, indien mogelijk, persoonsgegevens van klanten (of persoonsgegevens die laatstgenoemden verwerken) van gecontroleerde houders van cyberbeveiligingscertificaten of afgevers van conformiteitsverklaringen moeten worden gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met de AVG.

Voorts bepaalt de vierde paragraaf dat de in deze wet bedoelde uitwisseling tussen overheden geen betrekking mag hebben op persoonsgegevens van klanten (of persoonsgegevens die laatstgenoemden verwerken) van gecontroleerde houders van cyberbeveiligingscertificaten of afgevers van conformiteitsverklaringen.

De laatste paragraaf somt de categorieën van personen op die betrokken zijn bij verwerkingen van persoonsgegevens die plaatsvinden in het kader van de uitvoering van de Cyberbeveiligingsverordening of van deze wet.

Art. 37

Deze bepaling geeft uitvoering aan artikel 23 van Verordening EU 2016/679 (AVG). Om de openbare veiligheid en de bescherming van consumenten te waarborgen en in het kader van de doeleinden inzake het toezicht en de verwerking van klachten bedoeld in artikel 36, § 1, 2°, zijn de in artikel 12 tot 16, 18 en 19 van Verordening EU 2016/679 (AVG) bedoelde rechten van de betrokkenen niet van toepassing binnen de grenzen bepaald in het artikel.

De Gegevensbeschermingsautoriteit verklaart in haar advies dat er geen reden is om af te wijken van artikel 12 van de AVG, aangezien het niet om een recht van de betrokkenen gaat. Niettemin laat artikel 23, lid 1, van de AVG wel degelijk toe om af te wijken van dit artikel. De afwijking wordt dus behouden.

De uitzondering geldt alleen voor verwerkingen in het kader van het in artikel 36, § 1, 2°, bedoelde toezicht, voor zover de uitoefening van de rechten die zijn vastgelegd in de artikelen die het voorwerp uitmaken van de afwijking, nadelig zou zijn voor de controle of de voorbereidende werkzaamheden ervan. Alleen de nationale cyberbeveiligingscertificeringsautoriteit of de overheden die voor bepaalde toezichts- en sanctietaken door de Koning zijn aangewezen, kunnen, wanneer zij optreden als verwerkingsverantwoordelijke, gebruikmaken van deze uitzondering.

Le paragraphe 3 précise que cette limitation des droits ne vaut que sous réserve des principes de proportionnalité et de minimisation des données.

Le paragraphe 4 limite la période pendant laquelle il peut être dérogé aux droits des personnes précités.

Enfin, le paragraphe 5 établit les garde-fous nécessaires à l'application de la dérogation. Notamment, le délégué à la protection des données doit accuser réception des demandes liées à l'exercice des droits des personnes concernées et informer celles-ci du refus ou de la limitation de leur demande, sauf lorsque cela nuirait aux missions de supervision. Toute personne concernée ayant souhaité exercer ses droits doit, en tous les cas, être tenue informée une fois la dérogation levée.

Section 2

Durée de conservation

Art. 38

L'article 38 dispose que les données à caractère personnel traitées en exécution du projet de loi sont conservées 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 1er, sans préjudice des recours éventuels. Ce délai a été fixé ainsi afin de permettre la conservation de données à caractère personnel relatives à des schémas de certification de cybersécurité durant la période où des faits de fraude peuvent encore être poursuivis.

En effet, si les amendes administratives établies par le projet de loi se prescrivent par 3 ans, il apparaît nécessaire de s'assurer de conserver plus longtemps les données à caractère personnel pouvant être liées à un faux ou usage de faux relatif à une certification de cybersécurité. Ces infractions sont prescrites après 10 ans.

Paragraaf 3 bepaalt dat deze beperking van de rechten enkel geldt onder voorbehoud van het evenredigheidsbeginsel en het beginsel van minimale gegevensverwerking.

Paragraaf 4 beperkt de periode tijdens dewelke kan worden afgeweken van de rechten van voornoemde personen.

Tot slot bevat paragraaf 5 de nodige waarborgen voor de toepassing van de afwijking. De functionaris voor gegevensbescherming moet met name de ontvangst bevestigen van verzoeken in verband met de uitoefening van rechten van de betrokkenen en laatstgenoemden informeren over de weigering of beperking van hun verzoek, behalve wanneer dit nadelig zou zijn voor de toezichtsopdrachten. Iedere betrokkene die zijn rechten wenst uit te oefenen, moet alleszins op de hoogte worden gebracht zodra de afwijking is opgeheven.

Afdeling 2

Bewaartermijn

Art. 38

Artikel 38 bepaalt dat de in uitvoering van het wetsontwerp verwerkte persoonsgegevens 10 jaar worden bewaard na afloop van de verwerking die plaatsvond om een van de doeleinden bedoeld in artikel 36, § 1, te realiseren, onverminderd eventuele beroepsprocedures. Deze termijn maakt het mogelijk om persoonsgegevens betreffende cyberbeveiligingscertificeringsregelingen te bewaren tijdens de periode waarin fraudegevallen nog kunnen worden vervolgd.

Hoewel de administratieve geldboetes die in het wetsontwerp zijn bepaald na drie jaar verjaren, is het immers noodzakelijk dat persoonsgegevens die verband kunnen houden met valsheid of het gebruik van valse stukken betreffende een cyberbeveiligingscertificering langer worden bewaard. Deze inbreuken verjaren na 10 jaar.

CHAPITRE 9

Dispositions modificatives

Section 1re

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 39

L'article 39 insère, au sein de l'article 14, § 1, un 7° afin que l'Institut belge des services postaux et des télécommunications puisse exercer les missions de contrôle lui étant éventuellement confiées par le Roi conformément à l'article 5, § 2, de la loi.

Art. 40

Cette disposition clarifie le fait que la sécurité des réseaux et des systèmes d'information fait partie de la notion de sécurité publique afin de s'assurer que l'Institut belge des services postaux et des télécommunications puisse communiquer des informations confidentielles à l'autorité nationale de certification de cybersécurité ou à l'autorité visée à l'article 5, § 2.

L'article 14, § 2, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges énumère les autorités avec lesquelles les membres du Conseil et les membres du personnel de l'Institut belge des services postaux et des télécommunications peuvent communiquer des informations confidentielles dont ils ont eu connaissance dans le cadre de l'exercice de leur fonction. L'institut peut ainsi communiquer de telles informations aux services publics compétents en matière de sécurité publique.

Section 2

Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 41

Cette disposition met en place le régime dérogatoire de l'article 5, §§ 2 à 4, prévu en combinaison avec l'article 3, § 4, et auquel il est fait référence dans le commentaire de ce dernier.

Cette disposition insère à l'article 45 de la loi organique de la FSMA un paragraphe 6 habilitant le Roi, à la

HOOFDSTUK 9

Wijzigingsbepalingen

Afdeling 1

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 39

Artikel 39 voegt, in artikel 14, § 1, een punt 7° in zodat het Belgisch Instituut voor postdiensten en telecommunicatie de toezichtsopdrachten kan uitoefenen die hem eventueel zijn toevertrouwd door de Koning overeenkomstig artikel 5, § 2, van de wet.

Art. 40

Deze bepaling verduidelijkt dat de beveiliging van netwerk- en informatiesystemen onder het begrip "openbare veiligheid" valt om ervoor te zorgen dat het Belgisch Instituut voor postdiensten en telecommunicatie vertrouwelijke informatie kan delen met de nationale cyberbeveiligingscertificeringsautoriteit of de overheid bedoeld in artikel 5, § 2.

Artikel 14, § 2, 3°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector somt de overheden op waarmee de leden van de Raad en de personeelsleden van het Belgisch Instituut voor postdiensten en telecommunicatie vertrouwelijke informatie waarvan ze kennis hebben gekregen in het kader van de uitoefening van hun functie mogen uitwisselen. Zo mag het Instituut deze informatie delen met de openbare diensten die bevoegd zijn voor openbare veiligheid.

Afdeling 2

Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 41

Deze bepaling voert de afwijkende regeling van artikel 5, §§ 2 tot 4, in, die geldt in combinatie met artikel 3, § 4, en waarnaar wordt verwezen in de commentaar bij dit laatste artikel.

Deze bepaling voegt in artikel 45 van de organieke wet van de FSMA een paragraaf 6 in, die de Koning

demande de la FSMA et en fonction de l'objet du schéma de certification de cybersécurité concerné, à confier à la FSMA les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, en matière de contrôle et de sanctions des certifications européennes volontaires de cybersécurité de l'autorité nationale de certification de cybersécurité, à condition que la FSMA dispose de l'expertise requise. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée et la FSMA. Cette autorité n'exerce ces missions de contrôle qu'envers les entités visées au paragraphe 1er, 2°, de l'article 45 de sa loi organique.

Art. 42

Cet article vise à insérer une disposition dans la loi organique de la FSMA, afin de lui permettre de communiquer les informations confidentielles dont elle dispose à l'autorité nationale de certification de cybersécurité ou à une autre autorité désignée par le Roi, lorsque cela est nécessaire à l'application de la présente loi.

Section 3

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 43

Cet article vise à insérer une disposition dans la loi organique de la Banque nationale de Belgique, afin de lui permettre de communiquer les informations confidentielles dont elle dispose à l'autorité nationale de certification de cybersécurité ou à une autre autorité désignée par le Roi, lorsque cela est nécessaire à l'application de la présente loi.

Art. 44

Cette disposition met en place le régime dérogatoire à l'article 5, §§ 2 à 4 prévu en combinaison de l'article 3, § 5, auquel il est fait référence au commentaire de ce dernier. L'article 44 insère un article 36/48/1.

Ce qui a été exposé au commentaire de l'article 41 est applicable *mutatis mutandis* au régime institué par cet article, à la différence que la Banque nationale de Belgique n'exerce les missions de contrôle dont il est question qu'envers les entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12*bis* de sa loi

machtigt om, op verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling, de toezichts- en sanctieopdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, die de nationale cyberbeveiligingscertificeringsautoriteit met betrekking tot vrijwillige Europese cyberbeveiligingscertificeringen vervult, toe te vertrouwen aan de FSMA, op voorwaarde dat laatstgenoemde over de vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. Deze autoriteit vervult die toezichtsopdrachten enkel ten aanzien van de entiteiten bedoeld in paragraaf 1, 2°, van artikel 45 van haar organieke wet.

Art. 42

Dit artikel heeft tot doel een bepaling in te voegen in de organieke wet van de FSMA, waardoor deze de vertrouwelijke informatie waarover zij beschikt kan delen met de nationale cyberbeveiligingscertificeringsautoriteit of een andere door de Koning aangewezen overheid indien dit nodig is voor de toepassing van deze wet.

Afdeling 3

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 43

Dit artikel heeft tot doel een bepaling in te voegen in de organieke wet van de Nationale Bank van België, waardoor deze de vertrouwelijke informatie waarover zij beschikt kan delen met de nationale cyberbeveiligingscertificeringsautoriteit of een andere door de Koning aangewezen overheid indien dit nodig is voor de toepassing van deze wet.

Art. 44

Deze bepaling voert de afwijkende regeling van artikel 5, §§ 2 tot 4, in, die geldt in combinatie met artikel 3, § 5, en waarnaar wordt verwezen in de commentaar bij dit laatste artikel. Artikel 44 voegt een artikel 36/48/1 in.

De commentaar bij artikel 41 is *mutatis mutandis* van toepassing op de regeling die door dit artikel wordt ingevoerd, met dit verschil dat de Nationale Bank van België de betrokken toezichtsopdrachten enkel vervult ten aanzien van de entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12*bis* van haar organieke

organique et des lois particulières relatives au contrôle des établissements financiers.

Section 4

Modifications du Code de droit économique

Art. 45

Cet article vise à insérer une disposition dans le Code de droit économique afin que les termes “Règlement sur la cybersécurité” puissent y être régulièrement employés par la suite.

Art. 46

Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du SPF Économie en matière de certification de cybersécurité volontaire et de certification de cybersécurité rendue obligatoire en vertu du droit de l’Union ou du droit national.

Art. 47

Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du SPF Économie en matière de certification de cybersécurité volontaire.

Art. 48

L’article XV.30/3 précise que en matière de certification européenne de cybersécurité volontaire, le Roi peut confier, par arrêté délibéré en Conseil des ministres, certaines missions de contrôle et de sanction en matière de certification de cybersécurité (les missions visées aux chapitres 5 et 6 de la loi), à l’exception des articles 21 et 22, à des agents du SPF Économie moyennant plusieurs conditions cumulatives à savoir: le Roi doit solliciter l’avis de l’autorité nationale de certification de cybersécurité et le SPF Économie doit disposer de l’expertise requise.

Dans la mesure où il est dérogé à l’article 5, §§ 2 à 4, le Roi pourra également déterminer s’il entend confier ces missions aux agents du SPF Économie en procédant par schéma de certification de cybersécurité ou par toute autre forme (par exemple par entités ou produits faisant déjà l’objet d’une surveillance de la part du SPF Économie, etc.).

wet en de bijzondere wetten betreffende het toezicht op de financiële instellingen.

Afdeling 4

Wijzigingen van het Wetboek van economisch recht

Art. 45

Dit artikel heeft tot doel een bepaling in te voegen in het Wetboek van economisch recht, zodat de term “Cyberbeveiligingsverordening” daarna regelmatig kan worden gebruikt.

Art. 46

Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de bevoegdheden van de FOD Economie inzake de vrijwillige cyberbeveiligingscertificering en inzake de cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving.

Art. 47

Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de bevoegdheden van de FOD Economie inzake de vrijwillige cyberbeveiligingscertificering.

Art. 48

Artikel XV.30/3 bepaalt dat de Koning op het gebied van vrijwillige Europese cyberbeveiligingscertificering, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichts- en sanctieopdrachten op het gebied van cyberbeveiligingscertificering (de opdrachten bedoeld in hoofdstuk 5 en 6 van de wet), met uitzondering van artikel 21 en 22, kan toevertrouwen aan ambtenaren van de FOD Economie, onder verschillende cumulatieve voorwaarden, namelijk: de Koning moet het advies inwinnen van de nationale cyberbeveiligingscertificeringsautoriteit en de FOD Economie moet over de vereiste deskundigheid beschikken.

Voor zover afgeweken wordt van artikel 5, §§ 2 tot 4, kan de Koning ook bepalen of hij deze opdrachten wil toevertrouwen aan ambtenaren van de FOD Economie door te werk te gaan via een cyberbeveiligingscertificeringsregeling of via een andere vorm (bijvoorbeeld via entiteiten of producten die al onderworpen zijn aan het toezicht van de FOD Economie, etc.).

Cette attribution de compétences à des agents du SPF Économie n'est possible que dans la mesure où cette attribution est cohérente avec les compétences déjà détenues par le SPF Économie en vertu du Code de droit économique, de ses arrêtés d'exécution ou des règlements européens.

Art. 49

Cet article vise à insérer dans le livre XV du Code de droit économique, les dispositions relatives aux compétences du SPF Économie en matière de certification de cybersécurité obligatoire.

Art. 50

L'article 50 détermine les pouvoirs d'enquête, procédures et sanctions applicables dans le cadre de certifications européennes rendues obligatoires en vertu du droit de l'Union ou du droit national, à savoir ceux prévus dans le Code de droit économique. En ce qui concerne les sanctions, des articles sont introduits à cet effet dans ce Code par l'article 51.

L'article XV.30/5 précise que le Roi peut confier, par arrêté délibéré en Conseil des ministres, certaines missions de contrôle et de sanctions (à l'exception des articles 21 et 22 de la loi) en matière de certification européennes de cybersécurité à des agents du SPF Économie moyennant plusieurs conditions cumulatives à savoir: le Roi doit solliciter l'avis de l'autorité nationale de certification de cybersécurité et le SPF Économie dispose de l'expertise requise.

Les missions qui sont ainsi confiées au SPF Économie portent uniquement sur les tâches de contrôle et de sanctions mais ne portent pas atteinte aux autres chapitres de la loi. Les chapitres 1 à 4, 7 et 8 de la loi restent d'application pour les certifications européennes rendues obligatoires.

Art. 51

Cet article vise à déterminer les sanctions applicables en matière de certification obligatoire et fait la distinction entre les infractions qui seront punies d'amendes pénales de niveau 2 au sens de l'article XV.70 du Code de droit économique et celles, plus graves, qui seront punies d'amendes pénales de niveau 3 au sens de l'article XV.70 du même Code.

Deze toewijzing van bevoegdheden aan ambtenaren van de FOD Economie is slechts mogelijk voor zover ze aansluit bij de bevoegdheden waarover de FOD Economie al beschikt krachtens het Wetboek van economisch recht, de uitvoeringsbesluiten ervan of Europese verordeningen.

Art. 49

Dit artikel heeft tot doel in boek XV van het Wetboek van economisch recht de bepalingen in te voegen betreffende de bevoegdheden van de FOD Economie inzake de verplichte cyberbeveiligingscertificering.

Art. 50

Artikel 50 verduidelijkt de onderzoeksbevoegdheden, procedures en sancties die van toepassing zijn in het kader van Europese certificeringen die verplicht zijn op grond van de Europese of nationale wetgeving, namelijk deze vermeld in het Wetboek van economisch recht. Wat de sancties betreft, voegt artikel 51 daartoe artikelen in in dat Wetboek.

Artikel XV.30/5 bepaalt dat de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichts- en sanctieopdrachten (met uitzondering van artikel 21 en 22 van de wet) op het gebied van Europese cyberbeveiligingscertificering kan toevertrouwen aan ambtenaren van de FOD Economie, onder verschillende cumulatieve voorwaarden, namelijk: de Koning moet het advies inwinnen van de nationale cyberbeveiligingscertificeringsautoriteit en de FOD Economie moet over de vereiste expertise beschikken.

De opdrachten die aldus aan de FOD Economie worden toevertrouwd, hebben enkel betrekking op de taken inzake toezicht en sancties, maar doen geen afbreuk aan de andere hoofdstukken van de wet. De hoofdstukken 1 tot 4, 7 en 8 van de wet blijven van toepassing op verplichte Europese certificeringen.

Art. 51

Dit artikel heeft tot doel de sancties vast te stellen die van toepassing zijn op de verplichte certificering en maakt een onderscheid tussen inbreuken die met strafrechtelijke geldboetes van niveau 2 worden bestraft als bedoeld in artikel XV.70 van het Wetboek van economisch recht en zwaardere inbreuken die met strafrechtelijke geldboetes van niveau 3 worden bestraft als bedoeld in artikel XV.70 van hetzelfde Wetboek.

CHAPITRE 10

Entrée en vigueur

Art. 52

Cette disposition précise la date d'entrée en vigueur de la loi.

Le premier ministre,

Alexander DE CROO

Le ministre de l'Économie,

Pierre-Yves DERMAGNE

Le ministre des Finances, chargé de la Coordination de la lutte contre la fraude,

Vincent VAN PETEGHEM

La ministre des Télécommunications et de la Poste,

Petra DE SUTTER

HOOFDSTUK 10

Inwerkingtreding

Art. 52

Deze bepaling vermeldt de datum van inwerkingtreding van de wet.

De eerste minister,

Alexander DE CROO

De minister van Economie,

Pierre-Yves DERMAGNE

De minister van Financiën, belast met de coördinatie van de fraudebestrijding,

Vincent VAN PETEGHEM

De minister van Telecommunicatie en Post,

Petra DE SUTTER

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

Chapitre 1er

Définitions et dispositions générales

Section 1re

Objet et champ d'application

Sous-section 1re

Objet

Art. 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi met en œuvre partiellement le 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.

Sous-section 2

Champ d'application

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.

§ 2. Les chapitres 1 à 4 et 7, 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 d'une telle certification, 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 d'une telle certification.

§ 3. La présente loi ne porte pas préjudice aux mesures adoptées en droit belge pour protéger la sécurité publique, la

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteié

Hoofdstuk 1

Definities en algemene bepalingen

Afdeling 1

Onderwerp en toepassingsgebied

Onderafdeling 1

Onderwerp

Art. 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet geeft gedeeltelijk uitvoering aan 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.

Onderafdeling 2

Toepassingsgebied

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.

§ 2. De hoofdstukken 1 tot 4 en 7, alsook de artikelen 21 en 22, zijn ook van toepassing op een Europese cyberbeveiligingscertificering die wordt opgelegd.

Bij de uitvoering van artikel 21 en 22 in het kader van een dergelijke certificering zijn artikel 19 en 26 van toepassing.

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, de hoofdstuk 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van deze certificering.

§ 3. Deze wet doet geen afbreuk aan de maatregelen die in het Belgisch recht worden genomen ter bescherming van

défense, la sécurité nationale et les activités dans le domaine du droit pénal.

§ 4. 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 au sens de l'article 6, § 1er 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 ("loi NIS"), de l'article 3, 3° la loi du 1er juillet 2011 relative à la protection et la sécurité des infrastructures critiques et de l'article 2, 1° de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Dans le respect des dispositions légales applicables et du paragraphe 2, les autorités précitées et les services d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.

§ 5. L'article 5, §§ 2 à 4 n'est applicable ni à la Banque nationale de Belgique visée par la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique ni à la FSMA visée par 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.

Section 2

Définitions

Art. 4

Pour l'application de la présente loi, il faut entendre par:

1° "Règlement sur la cybersécurité": le 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;

2° "autorité nationale de certification de cybersécurité": l'autorité visée à l'article 58 du Règlement sur la cybersécurité et désignée par le Roi conformément à l'article 5, § 1er;

3° "GECC": Groupe européen de certification de cybersécurité visé à l'article 62 du Règlement sur la cybersécurité;

de openbare veiligheid, defensie, de nationale veiligheid en de activiteiten op het gebied van het strafrecht.

§ 4. 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 als bedoeld in artikel 6, § 1, 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 ("NIS-wet"), 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, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

Met inachtneming van de toepasselijke wettelijke bepalingen en van paragraaf 2 zorgen de voornoemde overheden en de bevoegde inspectiediensten voor het toezicht op en de sancties met betrekking tot verplichte Europese cyberbeveiligingscertificeringen.

§ 5. Artikel 5, §§ 2 tot 4, zijn 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.

Afdeling 2

Definities

Art. 4

Voor de toepassing van deze wet moet worden verstaan onder:

1° "Cyberbeveiligingsverordening": 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;

2° "nationale cyberbeveiligingscertificeringsautoriteit": de overheid bedoeld in artikel 58 van de Cyberbeveiligingsverordening en aangewezen door de Koning overeenkomstig artikel 5, § 1;

3° "EGC": Europese Groep voor cyberbeveiligingscertificering bedoeld in artikel 62 van de Cyberbeveiligingsverordening;

4° “autorité nationale d’accréditation”: l’organisme créé par le Roi en exécution de l’article VIII.30 du Code de droit économique et visée à l’article 2, 16° du Règlement sur la cybersécurité;

5° “autorité publique”: l’autorité publique au sens de l’article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel;

6° “service d’inspection”: le service d’inspection visé à l’article 13, § 1er.

Chapitre 2

Autorités compétentes et coopération au niveau national

Section 1re

Autorités compétentes

Art. 5

§ 1er. Le Roi désigne l’autorité qui est chargée, en tant qu’autorité nationale de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et par la présente loi.

§ 2. En fonction de l’objet du schéma de certification concerné et à la demande de l’autorité publique concernée, le Roi peut, par dérogation, confier, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6 de l’autorité visée à l’article 5, § 1er à une autre autorité publique, à l’exception des articles 21 et 22.

Le Roi veille à tenir compte de l’expertise de l’autorité publique concernée lors de l’attribution éventuelle de tâches de contrôle.

§ 3. Dans l’hypothèse visée au paragraphe 2, le Roi sollicite l’avis et se concerte au préalable avec l’autorité visée à l’article 5, § 1er et l’autorité publique concernée.

§ 4. Dans l’exercice de ces missions confiées par le Roi et sans préjudice de ses compétences légales en matière de contrôle et de sanctions, l’autorité publique concernée dispose des mêmes droits et obligations que ceux visés aux chapitres 5 et 6.

Section 2

Coopération au niveau national

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

4° “nationale accreditatieautoriteit”: instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;

5° “overheid”: de overheid als bedoeld in artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

6° “inspectiedienst”: de inspectiedienst bedoeld in artikel 13, § 1.

Hoofdstuk 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

Afdeling 1

Bevoegde autoriteiten

Art. 5

§ 1. De Koning wijst de autoriteit aan die, als nationale cyberbeveiligingscertificeringsautoriteit, belast is met de taken en opdrachten bedoeld in de Cyberbeveiligingsverordening en in deze wet.

§ 2. Naargelang het voorwerp van de betrokken certificeringsregeling en op verzoek van de betrokken overheid kan de Koning, bij wijze van afwijking en bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6 van de autoriteit bedoeld in artikel 5, § 1, volledig of gedeeltelijk toevertrouwen aan een andere overheid, met uitzondering van artikel 21 en 22.

De Koning houdt rekening met de expertise van de betrokken overheid bij de eventuele toekenning van toezichtstaken.

§ 3. In het in paragraaf 2 bedoelde geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, en de betrokken overheid.

§ 4. Bij de uitoefening van deze door de Koning toevertrouwde opdrachten en onverminderd haar wettelijke toezichts- en sanctiebevoegdheden beschikt de betrokken overheid over dezelfde rechten en verplichtingen als die bedoeld in hoofdstuk 5 en 6.

Afdeling 2

Samenwerking op nationaal niveau

Art. 6

§ 1. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen , voeren hun taken uit in overleg

avec les autorités publiques. 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. Les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne communiquent à l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi en vertu de l'article 5, § 2 toute information dont elle a besoin pour l'exécution de ses tâches.

§ 3. L'autorité visée à l'article 5, § 1er et les autorités publiques visées au paragraphe 1er s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou d'autres dispositions légales, notamment en matière de délivrance de certificat, de contrôle, de sanction et de réclamation. Les informations échangées se limitent à ce qui est pertinent et proportionnée à l'objectif de cet échange, notamment dans le respect 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). Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

§ 4. Les personnes dépositaires, par état ou par profession, 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, ainsi qu'éventuellement à d'autres autorités publiques lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.

Il s'agit notamment des informations nécessaires en matière de délivrance de certificat, de contrôle, de sanction et de réclamation. Les informations échangées se limitent à ce qui est pertinent et proportionnée à l'objectif de cet échange, notamment dans le respect 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). Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

Art. 7

Dans le cadre des missions et pouvoirs qui leur sont attribués par la loi, les autorités publiques peuvent assister l'autorité visée à l'article 5, § 1er dans ses missions de contrôle visées par la présente loi.

Chapitre 3

Autorité nationale de certification de cybersécurité

met de overheden. Naargelang het specifieke voorwerp van de certificeringsregeling kunnen de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, ook de private actoren raadplegen die betrokken zijn bij de cyberbeveiligingscertificering.

§ 2. Conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen verstrekken de autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, alle informatie die zij nodig heeft voor de uitvoering van haar taken.

§ 3. De autoriteit bedoeld in artikel 5, § 1, en de overheden bedoeld in paragraaf 1 wisselen onderling de informatie uit die nodig is voor de toepassing van de Cyberbeveiligingsverordening, van deze wet of van andere wettelijke bepalingen, met name wat betreft de afgifte van certificaten, het toezicht, sancties en klachten. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig 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). De modaliteiten van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

§ 4. Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, mogen deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, alsook eventueel aan andere overheden indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.

Het gaat met name om noodzakelijke informatie met betrekking tot de afgifte van certificaten, het toezicht, sancties en klachten. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig 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). De modaliteiten van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

Art. 7

De overheden mogen, in het kader van de opdrachten en bevoegdheden die hun zijn toevertrouwd door de wet, de autoriteit bedoeld in artikel 5, § 1, bijstaan bij de in deze wet bedoelde toezichtsopdrachten.

Hoofdstuk 3

Nationale cyberbeveiligingscertificeringsautoriteit

Section 1re

Représentation au Groupe européen de certification de cybersécurité

Art. 8

§ 1er. L'autorité visée à l'article 5, § 1er représente la Belgique au sein du GECC.

§ 2. Dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité visée à l'article 5, § 1er se concerte avec les autres autorités publiques désignées par le Roi, en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma de certification candidat au sens de l'article 49 du Règlement sur la cybersécurité.

§ 3. D'autres autorités publiques peuvent assister avec l'autorité visée à l'article 5, § 1er aux travaux et réunions du GECC.

Section 2

Indépendance

Art. 9

§ 1er. L'autorité visée à l'article 5, § 1er prend les mesures nécessaires afin d'assurer l'indépendance des membres de son personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de ses tâches de contrôle ou de certification en matière de cybersécurité, afin d'éviter des distorsions de concurrence et de garantir l'égalité de traitement de tous.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel de l'autorité visée à l'article 5, § 1er chargé de la certification ou du contrôle a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 2. Les membres du personnel de l'autorité visée à l'article 5, § 1er ne reçoivent ni ne cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

Chapitre 4

Délivrance des certificats européens

Afdeling 1

Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering

Art. 8

§ 1. De autoriteit bedoeld in artikel 5, § 1, vertegenwoordigt België in de EGC.

§ 2. In het kader van haar opdracht om België in de EGC te vertegenwoordigen overlegt de autoriteit bedoeld in artikel 5, § 1, met de andere door de Koning aangewezen overheden, met name bij de voorbereiding en goedkeuring van een advies over een potentiële certificeringsregeling als bedoeld in artikel 49 van de Cyberbeveiligingsverordening.

§ 3. Andere overheden kunnen, samen met de autoriteit bedoeld in artikel 5, § 1, de werkzaamheden en vergaderingen van de EGC bijwonen.

Afdeling 2

Onafhankelijkheid

Art. 9

§ 1. De autoriteit bedoeld in artikel 5, § 1, neemt de nodige maatregelen om, bij de uitvoering van haar toezichts- of certificeringstaken op het gebied van cyberbeveiliging, de onafhankelijkheid van haar personeelsleden te garanderen, belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen, teneinde vertekening van de mededinging te vermijden en de gelijke behandeling van allen te waarborgen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een met de certificering of het toezicht belast personeelslid van de autoriteit bedoeld in artikel 5, § 1, rechtstreeks of onrechtstreeks financiële, economische of andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 2. De personeelsleden van de autoriteit bedoeld in artikel 5, § 1, krijgen, noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze van niemand instructies.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

De Koning kan ook andere situaties benoemen als belangenconflicten.

Hoofdstuk 4

Afgifte van Europese certificaten

Section 1re

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élémentaire" ou "substantiel"

Art. 10

§ 1er. Les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel".

§ 2. Lorsque le schéma européen de certification de cybersécurité l'impose, la délivrance de tels certificats est réservée à l'autorité visée à l'article 5, § 1er.

§ 3. En fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er peut néanmoins déléguer en tout ou en partie la délivrance d'un certificat visé au paragraphe 2 à un organisme public accrédité par l'autorité nationale d'accréditation en tant qu'organisme d'évaluation de la conformité.

Section 2

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élevé"

Art. 11

§ 1er. L'autorité visée à l'article 5, § 1er délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé".

§ 2. En fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er peut toutefois déléguer en tout ou en partie cette tâche à un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation.

Section 3

Réclamation en cas de refus de délivrance

Art. 12

En cas de refus de délivrance du certificat, le demandeur peut introduire une réclamation devant l'autorité visée à l'article 5, § 1er selon les modalités prévues au chapitre 7.

Chapitre 5

Contrôle

Art. 13

§ 1er. L'autorité visée à l'article 5, § 1er dispose d'un service d'inspection qui peut à tout moment réaliser des contrôles du respect par les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens

Afdeling 1

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"

Art. 10

§ 1. De conformiteitsbeoordelingsinstanties die door de nationale accreditatieautoriteit geaccrediteerd zijn, geven de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af.

§ 2. Indien vereist door de Europese cyberbeveiligingscertificeringsregeling is de afgifte van deze certificaten voorbehouden aan de autoriteit bedoeld in artikel 5, § 1.

§ 3. Naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie kan de autoriteit bedoeld in artikel 5, § 1, de afgifte van een certificaat bedoeld in paragraaf 2 niettemin volledig of gedeeltelijk delegeren aan een overheidsinstelling die door de nationale accreditatieautoriteit als conformiteitsbeoordelingsinstantie geaccrediteerd is.

Afdeling 2

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"

Art. 11

§ 1. De autoriteit bedoeld in artikel 5, § 1, geeft de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" af.

§ 2. Naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie kan de autoriteit bedoeld in artikel 5, § 1, deze taak echter volledig of gedeeltelijk delegeren aan een conformiteitsbeoordelingsinstantie die door de nationale accreditatieautoriteit geaccrediteerd is.

Afdeling 3

Klacht ingeval de afgifte geweigerd wordt

Art. 12

Ingeval de afgifte van een certificaat geweigerd wordt, kan de aanvrager een klacht indienen bij de autoriteit bedoeld in artikel 5, § 1, volgens de in hoofdstuk 7 bepaalde modaliteiten.

Hoofdstuk 5

Toezicht

Art. 13

§ 1. De autoriteit bedoeld in artikel 5, § 1, beschikt over een inspectiedienst die op elk ogenblik controles kan uitvoeren om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten

volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le Règlement sur la cybersécurité, les schémas européens de certification de cybersécurité, la présente loi ou ses arrêtés d'exécution.

Dans l'exécution de ses tâches de contrôle, le service d'inspection agit de manière indépendante des autres services de l'autorité visée à l'article 5, § 1er, notamment du service chargé de la délivrance des certificats de cybersécurité.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande et précise le délai dans lequel les informations ou preuves doivent être fournies.

§ 3. En fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité, le service d'inspection peut faire appel à des experts, lesquels sont soumis aux règles de l'article 17.

Les frais de recours à des experts peuvent être mis à charge des organismes d'évaluation de la conformité, des titulaires de certificat de cybersécurité européen ou des émetteurs de déclaration de conformité de l'Union européenne.

Art. 14

Lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificat de cybersécurité européen volontaire ou un émetteur de déclaration de conformité de l'Union européenne est situé en dehors du territoire belge, le service d'inspection peut solliciter la coopération et l'assistance des autorités nationales de certification de cybersécurité compétentes de ces autres États.

Art. 15

§ 1er. Les membres assermentés du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres assermentés du service d'inspection ou les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les organismes d'évaluation de la conformité, titulaires de certificat de cybersécurité européen ou émetteurs de déclaration de conformité de l'Union européenne qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

§ 3. 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 disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission:

1° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen ou l'émetteur de déclaration de

en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de Cyberbeveiligingsverordening, de Europese cyberbeveiligingscertificeringsregelingen, deze wet of de uitvoeringsbesluiten ervan.

Bij de uitvoering van zijn toezichtstaken handelt de inspectiedienst onafhankelijk van de andere diensten van de autoriteit bedoeld in artikel 5, § 1, met name van de dienst belast met de afgifte van cyberbeveiligingscertificaten.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

§ 3. Naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling kan de inspectiedienst een beroep doen op experten, die onderworpen zijn aan de regels van artikel 17.

De kosten om een beroep te doen op experten kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen.

Art. 14

Wanneer een conformiteitsbeoordelingsinstantie, een houder van een vrijwillig Europees cyberbeveiligingscertificaat of een afgever van een EU-conformiteitsverklaring zich buiten het Belgische grondgebied bevindt, kan de inspectiedienst de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van deze andere landen om samenwerking en bijstand verzoeken.

Art. 15

§ 1. De beëdigde leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De beëdigde leden van de inspectiedienst of de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Ze leggen de eed af bij de leidend ambtenaar van hun dienst.

§ 3. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van hun opdracht:

1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de conformiteitsbeoordelingsinstantie, de houder van een Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring

conformité de l'Union européenne; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction;

2° prendre connaissance sur place et obtenir une copie du certificat ou de la déclaration de conformité de l'Union européenne, ainsi que de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission;

3° procéder à tout examen, contrôle et audition, et requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission;

4° relever et vérifier l'identité des personnes qui se trouvent sur les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen ou l'émetteur de déclaration de conformité de l'Union européenne 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° requérir l'assistance des services de la police fédérale ou locale.

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels les membres du personnel du service d'inspection souhaitent avoir accès;

2° les infractions présumées qui font l'objet du contrôle;

3° la législation qui donne lieu au contrôle pour lequel les inspecteurs estiment nécessaire d'obtenir une autorisation de visite;

4° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire;

5° la proportionnalité et la subsidiarité à l'égard de tout autre devoir d'enquête.

Le juge d'instruction décide dans un délai de 48 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. Le service d'inspection 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 assermentés du service d'inspection agissant conjointement.

gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter;

2° ter plaatse kennisnemen van het certificaat of de EU-conformiteitsverklaring, alsook van alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht en hiervan een kopie verkrijgen;

3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht;

4° de identiteit opnemen en controleren van de personen die zich bevinden op de plaatsen die de conformiteitsbeoordelingsinstantie, de houder van een Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring gebruikt 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° de bijstand vorderen van de federale of lokale politiediensten.

§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe de personeelsleden van de inspectiedienst toegang wensen te hebben;

2° de vermoedelijke inbreuken die het voorwerp zijn van de controle;

3° de wetgeving die aanleiding geeft tot de controle waarvoor de inspecteurs een machtiging tot bezoek menen nodig hebben;

4° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is;

5° de proportionaliteit en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

De onderzoeksrechter beslist binnen een termijn van maximum 48 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. De 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 beëdigde leden van de inspectiedienst die samen optreden.

§ 5. 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 à 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 personnel du service d'inspection qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 6. Les membres du service d'inspection peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 7. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 6, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection peut solliciter l'autorisation d'un juge d'instruction, selon les mêmes conditions que celles prévues au paragraphe 4.

§ 8. Lorsque cela s'avère nécessaire, les membres du service d'inspection disposent d'une habilitation de sécurité correspondant au niveau de classification, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, des informations auxquelles ils doivent avoir accès afin de réaliser leur contrôle.

§ 5. 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 geeft, 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 personeelsleden van de inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 6. De leden van de inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 7. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst de toestemming vragen van een onderzoeksrechter, volgens dezelfde voorwaarden als die bedoeld in paragraaf 4.

§ 8. Indien nodig beschikken de leden van de inspectiedienst over een veiligheidsmachtiging die overeenstemt met het classificatieniveau, als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de informatie waar zij toegang toe moeten hebben om hun controle uit te voeren.

Art. 16

§ 1er. À la fin des inspections, un rapport est dressé par le service d'inspection ou par l'autorité publique désignée par le Roi en vertu de l'article 5, § 2. Une copie de ce rapport est transmise à l'organisme d'évaluation de la conformité, au titulaire de certificat de cybersécurité européen ou à l'émetteur de déclaration de conformité de l'Union européenne inspecté.

§ 2. À sa demande et pour autant que cela poursuive l'accomplissement de ses missions légales, une autre autorité publique peut recevoir une copie du rapport prévu au § 1er.

§ 3. Par dérogation au paragraphe 2, 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 compétente lorsque celui-ci 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 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 ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Art. 17

§ 1er. Le service d'inspection limite l'accès aux informations relatives à l'exécution de ses missions aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente loi ou d'autres dispositions légales.

§ 2. Les membres du personnel du service d'inspection sont tenus au secret professionnel en ce qui concerne les informations en rapport à l'exécution de la présente loi.

§ 3. À sa demande et pour autant que cela poursuive l'accomplissement de ses missions légales, une autre autorité publique peut recevoir 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.

§ 4. 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 compétente 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 du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou 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.

§ 5. Dans l'exercice de leurs fonctions, les membres du personnel du service d'inspection peuvent:

Art. 16

§ 1. Na afloop van de inspecties stelt de inspectiedienst of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, een verslag op waarvan een kopie wordt bezorgd aan de geïnspecteerde conformiteitsbeoordelingsinstantie, houder van een Europees cyberbeveiligingscertificaat of afgever van een EU-conformiteitsverklaring.

§ 2. Op haar verzoek en voor zover dit nodig is voor het vervullen van haar wettelijke opdrachten kan een andere overheid een kopie krijgen van het verslag bedoeld in § 1.

§ 3. In afwijking van paragraaf 2 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 bevoegde sectorale overheid indien dit betrekking heeft op een controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in 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 of het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

Art. 17

§ 1. De inspectiedienst beperkt de toegang tot de informatie betreffende de uitvoering van zijn opdrachten tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet of andere wettelijke bepalingen.

§ 2. De personeelsleden van de inspectiedienst zijn gebonden aan het beroepsgeheim wat de informatie in verband met de uitvoering van deze wet betreft.

§ 3. Op haar verzoek en voor zover dit nodig is voor het vervullen van haar wettelijke opdrachten kan een andere overheid een kopie krijgen 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.

§ 4. De autoriteit bedoeld in artikel 5, § 1, of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, bezorgt de bevoegde sectorale overheid 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 wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of 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.

§ 5. Bij de uitoefening van hun functie mogen de personeelsleden van de inspectiedienst:

1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne leur est pas destinée personnellement;

2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;

3° prendre connaissance intentionnellement de données en matière de communications électroniques et relatives a une autre personne.

Art. 18

§ 1er. L'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen volontaire ou l'émetteur de déclaration de conformité de l'Union européenne apporte son entière collaboration aux membres du service d'inspection ou aux experts appelés à participer à l'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

Si nécessaire, l'organisme d'évaluation de la conformité, le titulaire de certificat de cybersécurité européen volontaire ou l'émetteur de déclaration de conformité de l'Union européenne met à disposition des membres du service d'inspection et des experts appelés à participer à l'inspection le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Après avis de l'autorité visée à l'article 5, § 1er, le Roi peut déterminer des rétributions relatives à la délivrance et aux prestations d'inspections réalisées dans le cadre du recours volontaire à des certifications et déclarations de conformité visées par le Règlement sur la cybersécurité.

Ces rétributions sont à charge des organismes d'évaluation de la conformité, titulaires de certificat de cybersécurité européen volontaire et des émetteurs de déclaration de conformité de l'Union européenne. Le Roi fixe les modalités de calcul et de paiement.

Chapitre 6

Sanctions

Section 1re

Procédure

Art. 19

§ 1er. Lorsqu'un ou plusieurs manquements aux exigences imposées par le Règlement sur la cybersécurité, la présente loi ou ses arrêtés d'exécution ou aux exigences de schémas de certification volontaire de cybersécurité sont constatés, le service d'inspection met en demeure le contrevenant de se conformer, dans un délai raisonnable qu'il fixe, aux obligations qui lui incombent.

1° met opzet kennisnemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hen bestemd is;

2° met opzet de personen identificeren die bij de overdracht van de informatie en de inhoud ervan betrokken zijn;

3° met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon.

Art. 18

§ 1. De conformiteitsbeoordelingsinstantie, de houder van een vrijwillig Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring verleent zijn volledige medewerking aan de leden van de inspectiedienst of de experten die deelnemen aan de inspectie bij de uitoefening van hun functie, met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de conformiteitsbeoordelingsinstantie, de houder van een vrijwillig Europees cyberbeveiligingscertificaat of de afgever van een EU-conformiteitsverklaring het nodige materiaal ter beschikking van de leden van de inspectiedienst en de experten die deelnemen aan de inspectie, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. Na advies van de autoriteit bedoeld in artikel 5, § 1, kan de Koning retributies bepalen voor de afgifte en de inspectieprestaties die geleverd worden in het kader van het vrijwillige gebruik van certificeringen en conformiteitsverklaringen bedoeld in de Cyberbeveiligingsverordening.

Deze retributies zijn ten laste van de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen. De Koning bepaalt de nadere regels inzake berekening en betaling.

Hoofdstuk 6

Sancties

Afdeling 1

Procedure

Art. 19

§ 1. Wanneer een of meer inbreuken op de voorschriften van de Cyberbeveiligingsverordening, deze wet of de uitvoeringsbesluiten ervan of op de voorschriften van vrijwillige cyberbeveiligingscertificeringsregelingen worden vastgesteld, maant de inspectiedienst de overtreder aan om zijn verplichtingen na te komen binnen een door hem vastgestelde redelijke termijn.

Le délai est déterminé en tenant compte des conditions de fonctionnement du contrevenant et des mesures à mettre en œuvre.

§ 2. Au préalable, le service d'inspection informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant son envoi par le service d'inspection.

Art. 20

§ 1er. Lorsque le service d'inspection constate que le contrevenant n'a pas respecté les obligations découlant de la loi ou du Règlement sur la cybersécurité, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection.

§ 2. Le fait pour quiconque d'empêcher ou entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté par les membres assermentés du service d'inspection dans un procès-verbal.

§ 3. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Section 2

Retrait d'un certificat

Art. 21

L'autorité visée à l'article 5, § 1er retire un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

Section 3

Limitation, suspension ou retrait d'une autorisation ou d'une délégation

Art. 22

L'autorité visée à l'article 5, § 1er limite, suspend ou retire les autorisations ainsi que les délégations qu'elle a accordées aux organismes d'évaluation de la conformité, lorsque le bénéficiaire de l'autorisation ou de la délégation ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

Section 4

De termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de overtreder en de te nemen maatregelen.

§ 2. De inspectiedienst deelt de overtreder vooraf, 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 vijftien 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 de zesde dag na de verzending ervan door de inspectiedienst.

Art. 20

§ 1. Als de inspectiedienst vaststelt dat de overtreder de verplichtingen van de wet of de Cyberbeveiligingsverordening niet is nagekomen, worden de feiten opgetekend in een procesverbaal door de beëdigde leden van de inspectiedienst.

§ 2. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 3. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Afdeling 2

Intrekking van een certificaat

Art. 21

De autoriteit bedoeld in artikel 5, § 1, trekt een cyberbeveiligingscertificaat in als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Afdeling 3

Beperken, opschorten of intrekken van een toelating of een delegatie

Art. 22

De autoriteit bedoeld in artikel 5, § 1, voorziet in de beperking, opschorting of intrekking van toelatingen alsook van delegaties die ze aan conformiteitsbeoordelingsinstanties heeft verleend, als de begunstigde van de toelating of delegatie de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Afdeling 4

Amendes administratives

Art. 23

§ 1er. Toute infraction au Règlement sur la cybersécurité, à la présente loi ou ses arrêtés d'exécution peut faire l'objet d'une sanction administrative.

§ 2. Est puni d'une amende de 500 à 75 000 euros quiconque ne répond pas à une demande d'information de l'autorité visée à l'article 5, § 1er.

§ 3. Est puni d'une amende de 500 à 100 000 euros le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC qui ne se conforme pas aux dispositions relatives à l'autoévaluation de la conformité visées à l'article 53 du Règlement sur la cybersécurité.

§ 4. Est également puni d'une amende de 500 à 100 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 5. Est puni d'une amende de 500 à 125 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "substantiel" ou "élevé" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 6. Est puni d'une amende de 500 à 150 000 euros quiconque ne coopère pas lors d'un contrôle, par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle.

§ 7. Est puni d'une amende de 500 à 200 000 euros quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi et de ses arrêtés d'exécution.

Art. 24

§ 1er. La décision d'imposer une amende administrative est motivée. Elle mentionne également le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité visée à l'article 5, § 1er informe au préalable le contrevenant de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les quinze jours de la réception de la proposition, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. La proposition est présumée reçue par le contrevenant le sixième jour suivant son envoi par de l'autorité visée à l'article 5, § 1er.

§ 3. En tenant compte des moyens de défense invoqués dans le délai visé au paragraphe 2 ou en l'absence de réaction du

Administratieve geldboetes

Art. 23

§ 1. Elke inbreuk op de Cyberbeveiligingsverordening, op deze wet of op de uitvoeringsbesluiten ervan kan aanleiding geven tot een administratieve sanctie.

§ 2. Wordt gestraft met een geldboete van 500 tot 75 000 euro: eenieder die niet reageert op een verzoek om informatie van de autoriteit bedoeld in artikel 5, § 1, van de wet.

§ 3. Wordt gestraft met een geldboete van 500 tot 100 000 euro: de fabrikant of aanbieder van ICT-producten, -diensten of -processen die niet voldoet aan de bepalingen inzake conformiteitszelfbeoordeling bedoeld in artikel 53 van de Cyberbeveiligingsverordening.

§ 4. Wordt eveneens gestraft met een geldboete van 500 tot 100 000 euro: de houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling.

§ 5. Wordt gestraft met een geldboete van 500 tot 125 000 euro: de houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling.

§ 6. Wordt gestraft met een geldboete van 500 tot 150 000 euro: eenieder die weigert mee te werken tijdens een inspectie, bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken.

§ 7. Wordt gestraft met een boete van 500 tot 200 000 euro: eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet en de uitvoeringsbesluiten ervan.

Art. 24

§ 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 autoriteit bedoeld in artikel 5, § 1, bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen vijftien 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 de zesde dag na de verzending ervan door de autoriteit bedoeld in artikel 5, § 1.

§ 3. Rekening houdend met de verweermiddelen die zijn aangevoerd binnen de in paragraaf 2 bedoelde termijn of bij

contrevenant dans ce même délai, l'autorité visée à l'article 5, § 1er peut adopter une sanction administrative visée à l'article 23.

§ 4. L'amende administrative est proportionnelle à la gravité, la durée, les moyens utilisés, les dommages causés et les circonstances des faits.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

§ 5. Le concours de plusieurs infractions peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 25

La décision est notifiée par envoi recommandé au contrevenant.

Une invitation à acquitter l'amende dans un délai d'un mois est jointe à la décision.

Art. 26

Le contrevenant peut contester la décision prise en vertu du chapitre 6 par l'autorité visée à l'article 5, § 1er devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1er.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Ce recours ne suspend pas l'exécution de la décision.

Art. 27

§ 1er. Lorsque le contrevenant reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité visée l'article 5, § 1er peut décerner une contrainte.

La contrainte est décernée par le représentant légal de l'autorité visée à l'article 5, § 1er ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les vingt-quatre heures, à peine d'exécution

gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de autoriteit bedoeld in artikel 5, § 1, een in artikel 23 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 van dezelfde feiten 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. 25

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. 26

De overtreder kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens hoofdstuk 6 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

De grond van de zaak wordt voorgelegd aan het Marktenhof, dat uitspraak doet met volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

Art. 27

§ 1. Als de overtreder de administratieve geldboete niet betaalt binnen de toegestane termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de autoriteit bedoeld in artikel 5, § 1, een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de autoriteit bedoeld in artikel 5, § 1, of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaardersexploot betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van

par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation à l'autorité visée à l'article 5, § 1er par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de la contrainte, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité visée à l'article 5, § 1er peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 28

L'autorité visée à l'article 5, § 1er ne peut imposer d'amende administrative à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis.

Chapitre 7

Réclamations

Section 1re

Saisine de l'autorité nationale de certification de cybersécurité

Art. 29

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 van de autoriteit bedoeld in artikel 5, § 1, van de wet bij deurwaardersexploot 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.

§ 4. De autoriteit bedoeld in artikel 5, § 1, 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.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 28

De autoriteit bedoeld in artikel 5, § 1, 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 7

Klachten

Afdeling 1

Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit

Art. 29

L'autorité visée à l'article 5, § 1er reçoit et traite les réclamations des personnes en rapport avec un certificat de cybersécurité européen, le refus de délivrance d'un certificat ou une déclaration de conformité de l'Union européenne.

Art. 30

Le dépôt d'une réclamation par toute personne physique ou morale au sens de l'article 63 du Règlement sur la cybersécurité est sans frais.

Art. 31

§ 1er. L'autorité compétente examine si la réclamation est recevable.

§ 2. Une réclamation est recevable lorsqu'elle:

— est rédigée dans l'une des langues nationales;

— contient un exposé des faits et les indications nécessaires pour identifier le certificat de cybersécurité européen, le refus de délivrance d'un certificat ou la déclaration de conformité de l'Union européenne sur laquelle elle porte;

— relève de la compétence de l'autorité visée à l'article 5, § 1er en vertu du Règlement sur la cybersécurité.

§ 3. L'autorité compétente peut inviter l'auteur de la réclamation à préciser sa réclamation.

Art. 32

L'affaire est traitée dans la langue nationale de la réclamation.

Art. 33

La décision portant sur la recevabilité de la réclamation est portée à la connaissance de l'auteur de la réclamation.

Si l'autorité visée à l'article 5, § 1er conclut à l'irrecevabilité de la réclamation, l'auteur de la réclamation en est informé par décision motivée.

Art. 34

Si l'autorité visée à l'article 5, § 1er conclut à la recevabilité de la réclamation, elle peut exercer les pouvoirs qui lui sont conférés conformément aux articles 11, 12, 21 et 22.

L'autorité visée à l'article 5, § 1er peut délivrer elle-même la certification demandée.

Section 2

Recours

Art. 35

De autoriteit bedoeld in artikel 5, § 1, ontvangt en behandelt klachten van personen over een Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of een EU-conformiteitsverklaring.

Art. 30

De indiening van een klacht door iedere natuurlijke of rechtspersoon als bedoeld in artikel 63 van de Cyberbeveiligingsverordening is kosteloos.

Art. 31

§ 1. De bevoegde autoriteit gaat na of de klacht ontvankelijk is.

§ 2. Een klacht is ontvankelijk wanneer zij:

— opgesteld is in een van de landstalen;

— een uiteenzetting van de feiten bevat, alsook de nodige indicaties voor de identificatie van het Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of de EU-conformiteitsverklaring waarop zij betrekking heeft;

— behoort tot de bevoegdheid van de autoriteit bedoeld in artikel 5, § 1, krachtens de Cyberbeveiligingsverordening.

§ 3. De bevoegde autoriteit kan de klager verzoeken zijn klacht toe te lichten.

Art. 32

De zaak wordt behandeld in de landstaal van de klacht.

Art. 33

De beslissing inzake de ontvankelijkheid van de klacht wordt ter kennis gebracht van de klager.

Indien de autoriteit bedoeld in artikel 5, § 1, de klacht onontvankelijk verklaart, wordt de klager hierover ingelicht door een met redenen omklede beslissing.

Art. 34

Indien de autoriteit bedoeld in artikel 5, § 1, de klacht ontvankelijk verklaart, kan zij de bevoegdheden uitoefenen die haar overeenkomstig de artikelen 11, 12, 21 en 22 zijn verleend.

De autoriteit bedoeld in artikel 5, § 1, kan zelf de gevraagde certificering afgeven.

Afdeling 2

Beroepen

Art. 35

Le réclamant peut contester la décision prise en vertu du chapitre 7 par l'autorité visée à l'article 5, § 1er devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1er.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Ce recours ne suspend pas l'exécution de la décision.

Chapitre 8

Dispositions finales

Section 1re

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 36

L'article 14, § 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, est complété par un 7° rédigé comme suit:

"7° L'Institut exerce les 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 [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]."

Art. 37

Dans l'article 14, § 2, 3°, g) de la même loi, inséré par la loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques (cité comme: loi Télécom), les mots "en ce compris la sécurité des réseaux et des systèmes d'information," sont insérés entre les mots "sécurité publique," et "ou de sécurité et protection civile".

De klager kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens hoofdstuk 7 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

De grond van de zaak wordt voorgelegd aan het Marktenhof, dat uitspraak doet met volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

Hoofdstuk 8

Slotbepalingen

Afdeling 1

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 36

Artikel 14, § 1, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector wordt aangevuld met een punt 7°, luidende:

"7° Het Instituut oefent 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 [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit]."

Art. 37

In artikel 14, § 2, 3°, g), van dezelfde wet, ingevoegd bij de wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische communicatie (aangehaald als: wet Telecom), worden de woorden "met inbegrip van de beveiliging van netwerk- en informatiesystemen," ingevoegd tussen de woorden "openbare veiligheid," en "of civiele veiligheid en bescherming".

Section 2

Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 38

L'article 45 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers est complété par un paragraphe 6, rédigé comme suit:

"§ 6. À la demande de la FSMA et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la FSMA, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er de la loi précitée et la FSMA. La FSMA exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu du paragraphe 1er, 2° du présent article et des lois particulières qui régissent le contrôle des établissements financiers."

Art. 39

L'article 75, § 1 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, est complété par un 26°, rédigé comme suit:

"26° à l'autorité visée à l'article 5, § 1er de la loi du […] 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."

Section 3

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique

Art. 40

Dans le Chapitre IV/4 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, inséré par la loi du 7 avril 2019 et modifié en dernier lieu par la loi du [date], il est inséré un article 36/48/1 rédigé comme suit:

"Art. 36/48/1. À la demande de la Banque et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la Banque, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux

Afdeling 2

Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 38

Artikel 45 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een paragraaf 6, luidende:

"§ 6. Op verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de FSMA toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. De FSMA vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens paragraaf 1, 2°, van dit artikel en de bijzondere wetten die het toezicht op de financiële instellingen regelen."

Art. 39

Artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een punt 26°, luidende:

"26° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van […] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet."

Afdeling 3

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 40

In Hoofdstuk IV/4 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij de wet van 7 april 2019 en het laatst gewijzigd bij de wet van [datum], wordt een artikel 36/48/1 ingevoegd, luidende:

"Art. 36/48/1. Op verzoek van de Bank en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5

chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er de la loi précitée et la Banque. La Banque exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12*bis* et des lois particulières qui régissent le contrôle des établissements financiers."

Art. 41

Dans l'article 36/14 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, modifié en dernier lieu par la loi du 20 juillet 2020, il est inséré un 20°/2 rédigé comme suit:

"20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er de la loi du […] 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;"

Section 4

Modification du Code de droit économique

Art. 42

L'article I.20 du Code de droit économique, inséré par la loi du 17 juillet 2013 et modifié par les lois du 1er décembre 2016 et du 15 avril 2018, est complété par un 9° rédigé comme suit:

"9° Règlement sur la cybersécurité: 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) no 526/2013.".

Art. 43

Dans le livre XV, titre Ier, chapitre 2, du même Code, inséré par la loi du 18 avril 2017, il est inséré une section 10 intitulée "Section 10. Certification de cybersécurité".

Art. 44

Dans la section 10, inséré par l'article 43, il est inséré une sous-section 1re intitulée "Sous-section 1re. Certification de cybersécurité volontaire".

en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de Bank toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de Bank. De Bank vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12*bis* en de bijzondere wetten die het toezicht op de financiële instellingen regelen."

Art. 41

In artikel 36/14 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, het laatst gewijzigd bij de wet van 20 juli 2020, wordt een punt 20°/2 ingevoegd, luidende:

"20° /2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van […] 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;"

Afdeling 4

Wijzigingen van het Wetboek van Economisch recht

Art. 42

Artikel I.20 van het Wetboek van Economisch recht, ingevoegd bij de wet van 17 juli 2013 en gewijzigd bij de wetten van 1 december 2016 en 15 april 2018, wordt aangevuld met een bepaling onder 9°, luidende:

"9° Cyberbeveiligingsverordening: 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. ".

Art. 43

In boek XV, titel 1, hoofdstuk 2, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, wordt een afdeling 10 ingevoegd, luidende "Afdeling 10 Certificering van de cyberbeveiliging".

Art. 44

In afdeling 10, ingevoegd bij artikel 43, wordt een onderafdeling 1 ingevoegd, luidende "Onderafdeling 1. Vrijwillige cyberbeveiligingscertificering".

Art. 45

Dans la sous-section 1re, inséré par l'article 44, il est inséré un article XV.30/3, rédigé comme suit:

"Art. XV.30/3. En matière de certification de cybersécurité volontaire, à la demande du SPF Économie, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [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], à certains agents du SPF Économie, à condition que le SPF Économie dispose de l'expertise requise à ces fins. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er de la loi précitée et avec le SPF Économie. Le SPF Économie exerce ces missions de contrôle uniquement sur les produits ou entités réglementés par le présent Code, ses arrêtés d'exécution ou les règlements de l'Union européenne relatifs aux matières qui, conformément aux livres VI, VII, IX et XII du présent Code, relèvent du pouvoir réglementaire du Roi.

Art. 46

Dans la section 10, inséré par l'article 43, il est inséré une sous-section 2 intitulée "Sous-section 2. Certification de cybersécurité obligatoire".

Art. 47

Par dérogation au paragraphe 2 de l'article 3 de la présente loi, il est inséré dans la sous-section 2, inséré par l'article 46, un article XV.30/4, rédigé comme suit:

"Art. XV.30/4. § 1. En matière de certification européenne de cybersécurité rendue obligatoire en vertu du droit de l'Union ou du droit national, à la demande du SPF Économie et après avis de l'autorité nationale de certification de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions en matière de contrôle relatives au règlement sur la cybersécurité ou relatives à la loi du [date] 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, à certains agents du SPF Économie, à condition que ce dernier dispose de l'expertise requise à ces fins.

§ 2. Les missions en matière de contrôle visées au paragraphe 1er, y compris la recherche, la constatation, la poursuite et la sanction des infractions, s'effectuent conformément aux dispositions du présent livre.

Art. 48

Dans le livre XV, titre 3, chapitre 2, section 11/3, du même Code, insérée par la loi du 18 avril 2017, sont insérés les articles XV.125/7 et XV.125/8, rédigés comme suit:

Art. 45

In onderafdeling 1, ingevoegd bij artikel 44, wordt een artikel XV.30/3 ingevoegd, luidende als volgt:

"Art. XV. 30/3. Op het gebied van vrijwillige cyberbeveiligingscertificering, op verzoek van de FOD Economie, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van de artikelen 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], aan bepaalde ambtenaren van de FOD Economie toevertrouwen, op voorwaarde dat de FOD Economie over de daarvoor vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FOD Economie. De FOD Economie vervult die toezichtsopdrachten enkel ten aanzien van producten of entiteiten die gereglementeerd zijn door dit Wetboek, de uitvoeringsbesluiten ervan of verordeningen van de Europese Unie betreffende aangelegenheden die, overeenkomstig de boeken VI, VII, IX en XII van dit Wetboek, tot de regelgevende bevoegdheid van de Koning behoren.

Art. 46

In afdeling 10, ingevoegd bij artikel 43, wordt een onderafdeling 2 ingevoegd, luidende "Onderafdeling 2. Verplichte cyberbeveiligingscertificering".

Art. 47

In afwijking van paragraaf 2 van artikel 3 van deze wet, wordt in onderafdeling 2, ingevoegd bij artikel 46, een artikel XV.30/4 ingevoegd, luidende als volgt:

"Art. XV.30/4. § 1. Met betrekking tot de Europese cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving, op verzoek van de FOD Economie en na advies van de nationale cyberbeveiligingscertificeringsautoriteit, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichtsopdrachten in verband met de Cyberbeveiligingsverordening of in verband met de wet van [datum] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, toevertrouwen aan bepaalde ambtenaren van de FOD Economie, op voorwaarde dat die laatste over de voor deze doeleinden vereiste expertise beschikt.

§ 2. De in het eerste paragraaf bedoelde controletaken, met inbegrip van de opsporing, vaststelling, vervolging en bestraffing van inbreuken, worden uitgeoefend overeenkomstig de bepalingen van dit boek.

Art. 48

In boek XV, titel 3, hoofdstuk 2, afdeling 11/3, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, worden de artikelen XV.125/7 en XV.125/8 ingevoegd, luidende:

"Art. XV.125/7. Dans le cadre de la surveillance visé à l'article [XV.30/4], sont punis d'une sanction de niveau 2:

1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;

2° quiconque ne coopère pas lors d'un contrôle, par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle.

Art. XV.125/8. Dans le cadre de la surveillance visé à l'article [XV.30/4], sont punis d'une sanction de niveau 3:

1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "substantiel" ou "élevé" qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;

2° quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité.".

Section 5

Entrée en vigueur et dispositions transitoires

Art. 49

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

"Art. XV.125/7. In het kader van het toezicht bedoeld in artikel [XV.30/4], wordt gestraft met een sanctie van niveau 2:

1° de houder van een cyberbeveiligingscertificaat die verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling;

2° eenieder die weigert mee te werken tijdens een inspectie, bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken.

Art. XV.125/8. In het kader van het toezicht bedoeld in artikel [XV.30/4], wordt gestraft met een sanctie van niveau 3:

de houder van een cyberbeveiligingscertificaat die verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken cyberbeveiligingscertificeringsregeling;

2° eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening.".

Afdeling 5

Inwerkingtreding en overgangsbepalingen

Art. 49

Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Formulaire AIR - v2 – oct. 2014

Analyse d'impact de la réglementation

RiA-AiR

:: Remplissez de préférence le formulaire en ligne ria-air.fed.be
:: Contactez le Helpdesk si nécessaire ria-air@premier.fed.be
:: Consultez le manuel, les FAQ, etc. www.simplification.be

Fiche signalétique

Auteur .a.

Membre du Gouvernement compétent	Premier Ministre
Contact cellule stratégique (nom, email, tél.)	info@premier.be
Administration compétente	Centre pour la Cybersécurité Belgique
Contact administration (nom, email, tél.)	legal@ccb.belgium.be

Projet .b.

Titre du projet de réglementation	Projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité	
Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.	Ce projet de loi vise à mettre en œuvre le Règlement (UE) 2019/881 (ci-après, le « Règlement européen »). Ce règlement européen exige l'adoption de dispositions en droit national afin de le mettre en œuvre, notamment pour les inspections, réclamations, recours, sanctions, collaboration entre autorités.	
Analyses d'impact déjà réalisées	☐ Oui ☒ Non	Si oui, veuillez joindre une copie ou indiquer la référence du document : _ _

Consultations sur le projet de réglementation .c.

Consultations obligatoires, facultatives ou informelles :	Inspecteur des Finances, Conseil des Ministres, avis du Conseil d'Etat, avis de l'Autorité de protection des données, avis du COC

Sources utilisées pour effectuer l'analyse d'impact .d.

Statistiques, documents de référence, organisations et personnes de référence :	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) no 526/2013 (règlement sur la cybersécurité)

Date de finalisation de l'analyse d'impact .e.

_

Formulaire AIR - v2 – oct. 2014

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

>

Un projet de réglementation aura généralement des impacts sur un nombre limité de thèmes.

Une liste non-exhaustive de mots-clés est présentée pour faciliter l'appréciation de chaque thème.

S'il y a des **impacts positifs et / ou négatifs, expliquez-les** (sur base des mots-clés si nécessaire) et indiquez les mesures prises pour alléger / compenser les éventuels impacts négatifs.

Pour les thèmes 3, 10, 11 et 21, des questions plus approfondies sont posées.

Consultez le manuel ou contactez le helpdesk ria-air@premier.fed.be pour toute question.

Lutte contre la pauvreté .1.

Revenu minimum conforme à la dignité humaine, accès à des services de qualité, surendettement, risque de pauvreté ou d'exclusion sociale (y compris chez les mineurs), illettrisme, fracture numérique.

☒ Impact positif ☐ Impact négatif ↓ Expliquez.

Accès à des services de qualité – Le Règlement européen mis en œuvre par le projet prévoit la mise en place d'une certification de cybersécurité volontaire de produits, services et processus relevant des technologies de l'information et des communcations (ci-après, « TIC »).Cette certification n'est possible qu'en respectant les règles établies par le schéma de certification concerné. Cela assure dès lors des produits, services et/ou processus TIC de qualité accrue car moins vulnérable aux cybermenaces.

☐ Pas d'impact

Égalité des chances et cohésion sociale .2.

Non-discrimination, égalité de traitement, accès aux biens et services, accès à l'information, à l'éducation et à la formation, écart de revenu, effectivité des droits civils, politiques et sociaux (en particulier pour les populations fragilisées, les enfants, les personnes âgées, les personnes handicapées et les minorités).

☐ Impact positif ☐ Impact négatif ↓ Expliquez.

_ _

☒ Pas d'impact

Égalité entre les femmes et les hommes .3.

Accès des femmes et des hommes aux ressources : revenus, travail, responsabilités, santé/soins/bien-être, sécurité, éducation/savoir/formation, mobilité, temps, loisirs, etc.

Exercice des droits fondamentaux par les femmes et les hommes : droits civils, sociaux et politiques.

1. Quelles personnes sont directement et indirectement concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

   Si aucune personne n'est concernée, expliquez pourquoi.

   Le projet porte sur la certification de cybersécurité de produits, services et processus TIC. Il ne porte pas et n'a pas d'impact sur l'égalité entre les femmes et les hommes.

↓ Si des personnes sont concernées, répondez à la question 2.

2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

_ _

↓ S'il existe des différences, répondez aux questions 3 et 4.

3. Certaines de ces différences limitent-elles l'accès aux ressources ou l'exercice des droits fondamentaux des femmes ou des hommes (différences problématiques) ? [O/N] > expliquez

_ _

4. Compte tenu des réponses aux questions précédentes, identifiez les impacts positifs et négatifs du projet sur l'égalité des femmes et les hommes ?

_ _

↓ S'il y a des impacts négatifs, répondez à la question 5.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

_ _

Santé .4.

Accès aux soins de santé de qualité, efficacité de l'offre de soins, espérance de vie en bonne santé, traitements des maladies chroniques (maladies cardiovasculaires, cancers, diabètes et maladies respiratoires chroniques), déterminants de la santé (niveau socio-économique, alimentation, pollution), qualité de la vie.

☒ Impact positif ☐ Impact négatif ↓ Expliquez. ☐ Pas d'impact

Accès aux soins de santé, efficacité de l'offre des soins (disponibilité) – L'accès aux, et l'offre de soins de santé est dépendant de produits, services et processus TIC. Dès lors, les hôpitaux ou professionnels des soins de santé qui ont recours à des produits, services ou processus TIC certifiés en matière de cybersécurité pour octroyer des soins sont moins vulnérables aux cybermenaces. Une meilleure résilience aux cybermenaces permet un meilleur accès aux soins de santé et une plus grande efficacité de ceux-ci.

Emploi .5.

Accès au marché de l'emploi, emplois de qualité, chômage, travail au noir, conditions de travail et de licenciement, carrière, temps de travail, bien-être au travail, accidents de travail, maladies professionnelles, équilibre vie privée - vie professionnelle, rémunération convenable, possibilités de formation professionnelle, relations collectives de travail.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Modes de consommation et production .6.

Stabilité/prévisibilité des prix, information et protection du consommateur, utilisation efficace des ressources, évaluation et intégration des externalités (environnementales et sociales) tout au long du cycle de vie des produits et services, modes de gestion des organisations.

☒ Impact positif ☐ Impact négatif ↓ Expliquez. ☐ Pas d'impact

Information et protection du consommateur – Les produits ou services certifiés pourront mettre en avant cette certification dans leur communication. Dès lors, les consommateurs seront informés des produits et/ou services plus résilient aux cybermenaces. En achetant des produits ou services certifiés, les consommateurs seront mieux protégés des cybermenaces.

Développement économique .7.

Création d'entreprises, production de biens et de services, productivité du travail et des ressources/matières premières, facteurs de compétitivité, accès au marché et à la profession, transparence du marché, accès aux marchés publics, relations commerciales et financières internationales, balance des importations/exportations, économie souterraine, sécurité d'approvisionnement des ressources énergétiques, minérales et organiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Investissements .8.

Investissements en capital physique (machines, véhicules, infrastructures), technologique, intellectuel (logiciel, recherche et développement) et humain, niveau d'investissement net en pourcentage du PIB.

☒ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

Investissements en capital technologique et intellectuel - L'investissement technologique et intellectuel pourra se faire avec plus d'informations quant aux exigences de cybersécurité respectées par les produits, services ou processus susceptibles de faire l'objet des investissements.

Recherche et développement .9.

Opportunités de recherche et développement, innovation par l'introduction et la diffusion de nouveaux modes de production, de nouvelles pratiques d'entreprises ou de nouveaux produits et services, dépenses de recherche et de développement.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

PME .10.

Impact sur le développement des PME.

1. Quelles entreprises sont directement et indirectement concernées par le projet ?
   Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (< 50 travailleurs) dont le % de micro-entreprise (< 10 travailleurs).
   Si aucune entreprise n'est concernée, expliquez pourquoi.
   Toute entreprise qui obtiendrait une certification de cybersécurité. Etant donné l'aspect volontaire de la certification et le fait que tous les secteurs reposent sur des produits, services ou processus TIC, il est impossible de préciser les secteurs, le nombre d'entreprises, un pourcentage de PME ou de micro-entreprises concernés.

↓ Si des PME sont concernées, répondez à la question 2.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.
   N.B. les impacts sur les charges administratives doivent être détaillés au thème 11
   >Impact positif : Compétitivité, sécurité - Assurance d'un certain niveau de cybersécurité acquis par le produit, service ou processus certifié.
   >Impact négatif : Coûts - Soumission à de potentielles inspections relatives au respect des exigences du schéma de certification de cybersécurité obtenu. L'inspection peut, par arrêté royal, comporter une rétribution pour les inspections.

↓ S'il y a un impact négatif, répondez aux questions 3 à 5.

3. Ces impacts sont-ils proportionnellement plus lourds sur les PME que sur les grandes entreprises ? [O/N] > expliquez
   Non, les inspections sont identiques pour toutes les entreprises.

4. Ces impacts sont-ils proportionnels à l'objectif poursuivi ? [O/N] > expliquez
   Oui, l'inspection est adaptée en fonction du niveau de sécurité de la certification concernée.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?
   Le projet prévoit que le service d'inspection exécute ses tâches de manière appropriée et nécessaire.

Charges administratives .11.

Réduction des formalités et des obligations administratives liées directement ou indirectement à l'exécution, au respect et/ou au maintien d'un droit, d'une interdiction ou d'une obligation.

↓ Si des citoyens (cf. thème 3) et/ou des entreprises (cf. thème 10) sont concernés, répondez aux questions suivantes.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.
   S'il n'y a aucune formalité ou obligation, expliquez pourquoi.

   a. Rien. Nouvelle réglementation.

   b. >Entreprise voulant déclarer une déclaration de conformité : Transmettre la déclaration de conformité de l'Union européenne à l'autorité nationale de certification de cybersécurité et à l'ENISA. Garder à la disposition de l'autorité nationale de certification de cybersécurité les informations pertinentes. Respecter les exigences du schéma de certification. Se soumettre aux inspections.
   >Entreprise voulant certifier un produit, service ou processus : Se soumettre à l'évaluation de l'entité compétente pour délivrer la certification. Garder à la disposition de l'autorité nationale de certification de cybersécurité les informations pertinentes. Respecter les exigences du schéma de certification. Se soumettre aux inspections.

↓ S'il y a des formalités et des obligations dans la réglementation actuelle*, répondez aux questions 2a à 4a.

↓ S'il y a des formalités et des obligations dans la réglementation en projet**, répondez aux questions 2b à 4b.

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

a. _ _*

b. Pour tous : Les informations permettant le contrôle du respect des schémas de certification de cybersécurité concerné.

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

a. _ _*

b. Pour tous : Sur demande du services d'inspection de l'autorité nationale de certification de cybersécurité.

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

a. _ _*

b. Pour tous : Périodicité égale à la période de validité de la certification. A ce terme, l'entreprise concernée doit à nouveau se soumettre à l'évaluation ou émettre une déclaration de conformité de l'Union européenne pour renouveler le certificat de cybersécurité. De plus, de manière aléatoire, sans périodicité précise, possibilité de contrôle.

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

Le projet prévoit que le service d'inspection exécute ses tâches de manière appropriée et nécessaire.

Énergie .12.

Mix énergétique (bas carbone, renouvelable, fossile), utilisation de la biomasse (bois, biocarburants), efficacité énergétique, consommation d'énergie de l'industrie, des services, des transports et des ménages, sécurité d'approvisionnement, accès aux biens et services énergétiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Mobilité .13.

Volume de transport (nombre de kilomètres parcourus et nombre de véhicules), offre de transports collectifs, offre routière, ferroviaire, maritime et fluviale pour les transports de marchandises, répartitions des modes de transport (modal shift), sécurité, densité du trafic.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Alimentation .14.

Accès à une alimentation sûre (contrôle de qualité), alimentation saine et à haute valeur nutritionnelle, gaspillages, commerce équitable.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Changements climatiques .15.

Émissions de gaz à effet de serre, capacité d'adaptation aux effets des changements climatiques, résilience, transition énergétique, sources d'énergies renouvelables, utilisation rationnelle de l'énergie, efficacité énergétique, performance énergétique des bâtiments, piégeage du carbone.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Ressources naturelles .16.

Gestion efficiente des ressources, recyclage, réutilisation, qualité et consommation de l'eau (eaux de surface et souterraines, mers et océans), qualité et utilisation du sol (pollution, teneur en matières organiques, érosion, assèchement, inondations, densification, fragmentation), déforestation.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Air intérieur et extérieur .17.

Qualité de l'air (y compris l'air intérieur), émissions de polluants (agents chimiques ou biologiques : méthane, hydrocarbures, solvants, SOx, NOx, NH3), particules fines.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Biodiversité .18.

Niveaux de la diversité biologique, état des écosystèmes (restauration, conservation, valorisation, zones protégées) , altération et fragmentation des habitats, biotechnologies, brevets d'invention sur la matière biologique, utilisation des ressources génétiques, services rendus par les écosystèmes (purification de l'eau et de l'air, …), espèces domestiquées ou cultivées, espèces exotiques envahissantes, espèces menacées.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Nuisances .19.

Nuisances sonores, visuelles ou olfactives, vibrations, rayonnements ionisants, non ionisants et électromagnétiques, nuisances lumineuses.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Autorités publiques .20.

Fonctionnement démocratique des organes de concertation et consultation, services publics aux usagers, plaintes, recours, contestations, mesures d'exécution, investissements publics.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Cohérence des politiques en faveur du développement .21.

Prise en considération des impacts involontaires des mesures politiques belges sur les intérêts des pays en développement.

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants :

   - o sécurité alimentaire
   - o santé et accès aux médicaments
   - o travail décent
   - o commerce local et international
   - o revenus et mobilisations de ressources domestiques (taxation)
   - o mobilité des personnes
   - o environnement et changements climatiques (mécanismes de développement propre)
   - o paix et sécurité

   Expliquez si aucun pays en développement n'est concerné.

   L'avant-projet de loi ne concerne pas les pays en développement. L'avant-projet concerne la Belgique.

↓ S'il y a des impacts positifs et/ou négatifs, répondez à la question 2.

2. Précisez les impacts par groupement régional ou économique (lister éventuellement les pays). Cf. manuel

_ _

↓ S'il y a des impacts négatifs, répondez à la question 3.

3. Quelles mesures sont prises pour les alléger / compenser les impacts négatifs ?

_ _

RIA formulier - v2 - oct. 2014

Regelgevingsimpactanalyse

RiA-AiR

:: Vul het formulier bij voorkeur online in ria-air.fed.be
:: Contacteer de helpdesk indien nodig ria-air@premier.fed.be
:: Raadpleeg de handleiding, de FAQ, enz. www.vereenvoudiging.be

Beschrijvende fiche

Auteur .a.

Bevoegd regeringslid	Eerste Minister
Contactpersoon beleidscel (Naam, E-mail, Tel. Nr.)	info@premier.be
Overheidsdienst	Centrum voor Cybersecurity België
Contactpersoon overheidsdienst (Naam, E-mail, Tel. Nr.)	legal@ccb.belgium.be

Ontwerp .b.

Titel van het ontwerp van regelgeving	Ontwerp van wet inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit
Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.	Dit wetsontwerp geeft uitvoering aan Verordening (EU) 2019/881 (hierna, de "Europese Verordening"). Om deze Europese Verordening uit te voeren, moeten bepalingen worden ingevoerd in het nationaal recht, met name voor inspecties, klachten, beroepen, sancties en de samenwerking tussen overheden.
Impactanalyses reeds uitgevoerd	☐ Ja ☒ Nee — Indien ja, gelieve een kopie bij te voegen of de referentie van het document te vermelden: _ _

Raadpleging over het ontwerp van regelgeving .c.

Verplichte, facultatieve of informele raadplegingen:	Inspecteur van Financiën, Ministerraad, advies van de Raad van State, advies Gegevensbeschermingsautoriteit, advies COC.

Bronnen gebruikt om de impactanalyse uit te voeren .d.

Statistieken, referentiedocumenten, organisaties en contactpersonen:	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)

Datum van beëindiging van de impactanalyse .e.

23/05/2022

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

>

Een ontwerp van regelgeving zal meestal slechts impact hebben op enkele thema's.

Een niet-exhaustieve lijst van trefwoorden is gegeven om de inschatting van elk thema te vergemakkelijken.

Indien er een **positieve en/of negatieve impact** is, leg deze uit (gebruik indien nodig trefwoorden) en vermeld welke maatregelen worden genomen om de eventuele negatieve effecten te verlichten/te compenseren.

Voor de thema's 3, 10, 11 en 21, worden meer gedetailleerde vragen gesteld.

Raadpleeg de handleiding of contacteer de helpdesk ria-air@premier.fed.be indien u vragen heeft.

Kansarmoedebestrijding .1.

Menswaardig minimuminkomen, toegang tot kwaliteitsvolle diensten, schuldenoverlast, risico op armoede of sociale uitsluiting (ook bij minderjarigen), ongeletterdheid, digitale kloof.

☒ Positieve impact ☐ Negatieve impact ↓ Leg uit.

Toegang tot kwaliteitsvolle diensten – De Europese Verordening die is uitgevoerd door het ontwerp voorziet in de invoering van een vrijwillige cyberbeveiligingscertificering van producten, diensten en processes van de informatie- en communicatietechnologie (hierna, "ICT"). Deze certificering is enkel mogelijk mits naleving van de regels van het betrokken certificeringsschema. Dit garandeert dus ICT-producten, -diensten en/of processen van betere kwaliteit, want ze zijn minder kwetsbaar voor cyberdreigingen.

☐ Geen impact

Gelijke Kansen en sociale cohesie .2.

Non-discriminatie, gelijke behandeling, toegang tot goederen en diensten, toegang tot informatie, tot onderwijs en tot opleiding, loonkloof, effectiviteit van burgerlijke, politieke en sociale rechten (in het bijzonder voor kwetsbare bevolkingsgroepen, kinderen, ouderen, personen met een handicap en minderheden).

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit.

_ _

☒ Geen impact

Gelijkheid van vrouwen en mannen .3.

Toegang van vrouwen en mannen tot bestaansmiddelen: inkomen, werk, verantwoordelijkheden, gezondheid/zorg/welzijn, veiligheid, opleiding/kennis/vorming, mobiliteit, tijd, vrije tijd, etc.

Uitoefening door vrouwen en mannen van hun fundamentele rechten: burgerlijke, sociale en politieke rechten.

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

   Indien geen enkele persoon betrokken is, leg uit waarom.

   Het ontwerp heeft betrekking op de certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen. Het heeft geen betrekking op de gelijkheid van vrouwen en mannen en heeft er geen impact op.

↓ Indien er personen betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

   _ _

↓ Indien er verschillen zijn, beantwoord dan vragen 3 en 4.

3. Beperken bepaalde van deze verschillen de toegang tot bestaansmiddelen of de uitoefening van fundamentele rechten van vrouwen of mannen (problematische verschillen)? [J/N] > Leg uit

   _ _

4. Identificeer de positieve en negatieve impact van het ontwerp op de gelijkheid van vrouwen en mannen, rekening houdend met de voorgaande antwoorden?

_ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 5.

5. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

_ _

Gezondheid .4.

Toegang tot kwaliteitsvolle gezondheidszorg, efficiëntie van het zorgaanbod, levensverwachting in goede gezondheid, behandelingen van chronische ziekten (bloedvatenziekten, kankers, diabetes en chronische ademhalingsziekten), gezondheidsdeterminanten (sociaaleconomisch niveau, voeding, verontreiniging), levenskwaliteit.

☒ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

Toegang tot de gezondheidzorg, efficiëntie van het zorgaanbod (beschikbaarheid) – De toegang tot de gezondheidzorg en het zorgaanbod zijn afhankelijk van ICT-producten, -diensten en -processen. De ziekenhuizen of gezondheidszorgbeoefenaars die bij het verstrekken van zorg gebruikmaken van ICT-producten, -diensten of -processen die gecertificeerd zijn op het vlak van cyberbeveiliging zijn minder kwetsbaar voor cyberdreigingen. Een betere veerkracht tegenover cyberdreigingen verbetert de toegang tot de gezondheidzorg en maakt deze efficiënter.

Werkgelegenheid .5.

Toegang tot de arbeidsmarkt, kwaliteitsvolle banen, werkloosheid, zwartwerk, arbeids- en ontslagomstandigheden, loopbaan, arbeidstijd, welzijn op het werk, arbeidsongevallen, beroepsziekten, evenwicht privé- en beroepsleven, gepaste verloning, mogelijkheid tot beroepsopleiding, collectieve arbeidsverhoudingen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Consumptie- en productiepatronen .6.

Prijsstabiliteit of -voorzienbaarheid, inlichting en bescherming van de consumenten, doeltreffend gebruik van hulpbronnen, evaluatie en integratie van (sociale- en milieu-) externaliteiten gedurende de hele levenscyclus van de producten en diensten, beheerpatronen van organisaties.

☒ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

Voorlichting en bescherming van de consument - De gecertifieerde producten of diensten zullen deze certificering in hun communicatie kunnen aanvoeren. Dus zullen de consumenten op de hoogte zijn van de producten en/of diensten die de beste veerkracht bieden ten opzichte van cyberdreigingen. Door gecertificeerde producten of diensten te kopen zijn de consumenten beter beschermd tegen cyberdreigingen.

Economische ontwikkeling .7.

Oprichting van bedrijven, productie van goederen en diensten, arbeidsproductiviteit en productiviteit van hulpbronnen/grondstoffen, competitiviteitsfactoren, toegang tot de markt en tot het beroep, markttransparantie, toegang tot overheidsopdrachten, internationale handels- en financiële relaties, balans import/export, ondergrondse economie, bevoorradingszekerheid van zowel energiebronnen als minerale en organische hulpbronnen.

☐ Positieve impact ☒ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Investeringen .8.

Investeringen in fysiek (machines, voertuigen, infrastructuren), technologisch, intellectueel (software, onderzoek en ontwikkeling) en menselijk kapitaal, nettoinvesteringscijfer in procent van het bbp.

☒ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

Investeringen in technologisch en intellectueel kapitaal – De technologische en intellectuele investering zal uitgevoerd kunnen worden met meer informatie betreffende de cyberbeveiligingsvereisten die nageleefd worden door de producten, diensten of processen waarin geïnvesteerd kan worden.	

Onderzoek en ontwikkeling .9.

Mogelijkheden betreffende onderzoek en ontwikkeling, innovatie door de invoering en de verspreiding van nieuwe productiemethodes, nieuwe ondernemingspraktijken of nieuwe producten en diensten, onderzoeks- en ontwikkelingsuitgaven.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Kmo's .10.

Impact op de ontwikkeling van de kmo's.

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?
   Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (< 50 werknemers), waaronder het % micro-ondernemingen (< 10 werknemers).
   Indien geen enkele onderneming betrokken is, leg uit waarom.
   Elke onderneming die een cyberbeveiligingscertificering krijgt. Gezien het vrijwillige aspect van de certificering en het feit dat alle sectoren gebaseerd zijn op ICT-producten, - diensten of -processen, is het onmogelijk om de betrokken sectoren, het aantal ondernemingen, het percentage kmo's of micro-ondernemingen te specificeren.

↓ Indien er kmo's betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.
   N.B. De impact op de administratieve lasten moet bij thema 11 gedetailleerd worden.
   >Positieve impact: concurrentievermogen, veiligheid – Garantie op een bepaald niveau van cyberbeveiliging behaald door het gecertificeerde product, dienst of proces.
   >Negatieve impact: Kostprijs - Onderwerping aan mogelijke inspecties in verband met de naleving van de vereisten van het verkregen cyberbeveiligingscertificeringsschema. De inspectie kan bij koninklijk besluit een vergoeding voor de inspecties inhouden.

↓ Indien er een negatieve impact is, beantwoord dan vragen 3 tot 5.

3. Is deze impact verhoudingsgewijs zwaarder voor de kmo's dan voor de grote ondernemingen? [J/N] > Leg uit
   Nee, de inspecties zijn identiek voor alle ondernemingen.

4. Staat deze impact in verhouding tot het beoogde doel? [J/N] > Leg uit
   Ja, de inspectie is aangepast in functie van het veiligheidsniveau van de betrokken certificering.

5. Welke maatregelen worden genomen om deze negatieve impact te verlichten / te compenseren?
   Het ontwerp voorziet erin dat de inspectiedienst zijn taken uitvoert op proportionele en noodzakelijke wijze.

Administratieve lasten .11.

Verlaging van de formaliteiten en administratieve verplichtingen die direct of indirect verbonden zijn met de uitvoering, de naleving en/of de instandhouding van een recht, een verbod of een verplichting.

↓ Indien burgers (zie thema 3) en/of ondernemingen (zie thema 10) betrokken zijn, beantwoord dan volgende vragen.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.
   Indien er geen enkele formaliteiten of verplichtingen zijn, leg uit waarom.

   a. Niets. Nieuwe regelgeving.

   b. >Onderneming die een conformiteitsverklaring wil afleggen: de EU-conformiteitsverklaring overmaken aan de nationale cyberbeveiligingscertificeringsautoriteit en aan ENISA. Relevante informatie ter beschikking houden voor de nationale cyberbeveiligingscertificeringsautoriteit. Zich houden aan de vereisten van het

certificeringsschema. Zich onderwerpen aan de inspecties.
>Onderneming die een product, dienst of proces willen certificeren: zich onderwerpen aan de evaluatie van de bevoegde entiteit om de certificering uit te reiken. Relevante informatie ter beschikking houden van de nationale cyberbeveiligingscertificeringsautoriteit. Zich houden aan de vereisten van het certificeringsschema. Zich onderwerpen aan de inspecties.

↓ Indien er formaliteiten en/of verplichtingen zijn in de huidige* regelgeving, beantwoord dan vragen 2a tot 4a.

↓ Indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving**, beantwoord dan vragen 2b tot 4b.

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?

a. _ _*

b. Voor allen: de informatie die de controle van de naleving van het betrokken certificeringsschema mogelijk maken.

3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?

a. _ _*

b. Voor allen: Op verzoek van de inspectiediensten van de nationale cyberbeveiligingscertificeringsautoriteit.

4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?

a. _ _*

b. Voor allen: periodiciteit gelijk aan de geldigheidsduur van de certificering. Op het einde van deze duur moet de betrokken onderneming zich opnieuw aan een evaluatie onderwerpen of een EU-conformiteitsverklaring afgeven om het cyberbeveiligingscertificaat te verlengen. Bovendien bestaat de mogelijkheid op controle, op willekeurige basis, zonder duidelijke periodiciteit.

5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?

Het ontwerp voorziet erin dat de inspectiedienst zijn taken uitvoert op gepaste en noodzakelijk wijze.

Energie .12.

Energiemix (koolstofarm, hernieuwbaar, fossiel), gebruik van biomassa (hout, biobrandstoffen), energie-efficiëntie, energieverbruik van de industrie, de dienstensector, de transportsector en de huishoudens, bevoorradingszekerheid, toegang tot energiediensten en -goederen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Mobiliteit .13.

Transportvolume (aantal afgelegde kilometers en aantal voertuigen), aanbod van gemeenschappelijk personenvervoer, aanbod van wegen, sporen en zee- en binnenvaart voor goederenvervoer, verdeling van de vervoerswijzen (modal shift), veiligheid, verkeersdichtheid.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Voeding .14.

Toegang tot veilige voeding (kwaliteitscontrole), gezonde en voedzame voeding, verspilling, eerlijke handel.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Klimaatverandering .15.

Uitstoot van broeikasgassen, aanpassingsvermogen aan de gevolgen van de klimaatverandering, veerkracht, energie overgang, hernieuwbare energiebronnen, rationeel energiegebruik, energie-efficiëntie, energieprestaties van gebouwen, winnen van koolstof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Natuurlijke hulpbronnen .16.

Efficiënt beheer van de hulpbronnen, recyclage, hergebruik, waterkwaliteit en -consumptie (oppervlakte- en grondwater, zeeën en oceanen), bodemkwaliteit en -gebruik (verontreiniging, organisch stofgehalte, erosie, drooglegging, overstromingen, verdichting, fragmentatie), ontbossing.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Buiten- en binnenlucht .17.

Luchtkwaliteit (met inbegrip van de binnenlucht), uitstoot van verontreinigende stoffen (chemische of biologische agentia: methaan, koolwaterstoffen, oplosmiddelen, SOX, NOX, NH3), fijn stof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

_ _

Biodiversiteit .18.

Graad van biodiversiteit, stand van de ecosystemen (herstelling, behoud, valorisatie, beschermde zones), verandering en fragmentatie van de habitatten, biotechnologieën, uitvindingsoctrooien in het domein van de biologie, gebruik van genetische hulpbronnen, diensten die de ecosystemen leveren (water- en luchtzuivering, enz.), gedomesticeerde of gecultiveerde soorten, invasieve uitheemse soorten, bedreigde soorten.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☐ Geen impact

_ _

Hinder .19.

Geluids-, geur- of visuele hinder, trillingen, ioniserende, niet-ioniserende en elektromagnetische stralingen, lichtoverlast.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Overheid .20.

Democratische werking van de organen voor overleg en beraadslaging, dienstverlening aan gebruikers, klachten, beroep, protestbewegingen, wijze van uitvoering, overheidsinvesteringen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Beleidscoherentie ten gunste van ontwikkeling .21.

Inachtneming van de onbedoelde neveneffecten van de Belgische beleidsmaatregelen op de belangen van de ontwikkelingslanden.

RIA formulier - v2 - oct. 2014

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van:

- o voedselveiligheid
- o gezondheid en toegang tot geneesmiddelen
- o waardig werk
- o lokale en internationale handel
- o inkomens en mobilisering van lokale middelen (taxatie)
- o mobiliteit van personen
- o leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling)
- o vrede en veiligheid

Indien er geen enkelen ontwikkelingsland betrokken is, leg uit waarom.

Dit ontwerp heeft geen betrekking op de ontwikkelingslanden. Het betreft België.

↓ Indien er een positieve en/of negatieve impact is, beantwoord dan vraag 2.

2. Verduidelijk de impact per regionale groepen of economische categorieën (eventueel landen oplijsten). Zie bijlage

_ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 3.

3. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

_ _

AVIS DU CONSEIL D'ÉTAT N° 69.813/2/V DU 30 AOUT 2021

Le 5 juillet 2021, le Conseil d'État, section de législation, a été invité par le Premier ministre à communiquer un avis, dans un délai de trente jours prorogé de plein droit* jusqu'au 19 août 2021, sur un avant-projet de loi "relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité".

L'avant-projet a été examiné par la deuxième chambre des vacations le 30 août 2021. La chambre était composée de Pierre Vandernoot, président de chambre, Bernard Blero et Christine Horevoets, conseillers d'État, Sébastien Van Drooghenbroeck, assesseur, et Béatrice Drapier, greffier.

Le rapport a été présenté par Roger Wimmer, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Vandernoot.

L'avis, dont le texte suit, a été donné le 30 août 2021.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, 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.

Observations générales

1. Le dossier joint à la demande d'avis ne comprenait pas d'explications détaillées quant au lien entre chacune des dispositions de l'avant-projet et celles 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

* Ce délai résulte de l'article 84, § 1er, alinéa 1er, 2°, *in fine*, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973 qui précise que ce délai est prolongé de plein droit de quinze jours lorsqu'il prend cours du 15 juillet au 31 juillet ou lorsqu'il expire entre le 15 juillet et le 15 août.

‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

ADVIES VAN DE RAAD VAN STATE NR. 69.813/2/V VAN 30 AUGUSTUS 2021

Op 5 juli 2021 is de Raad van State, afdeling Wetgeving, door de Eerste minister verzocht binnen een termijn van dertig dagen van rechtswege* verlengd tot 19 augustus 2021 een advies te verstrekken over een voorontwerp van wet "inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit".

Het voorontwerp is door de tweede vakantiekamer onderzocht op 30 augustus 2021. De kamer was samengesteld uit Pierre Vandernoot, kamervoorzitter, Bernard Blero en Christine Horevoets, staatsraden, Sébastien Van Drooghenbroeck, assessor, en Béatrice Drapier, griffier.

Het verslag is uitgebracht door Roger Wimmer, eerste auditeurs.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre Vandernoot.

Het advies, waarvan de tekst hierna volgt, is gegeven op 30 augustus 2021.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, 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 ontwerp,‡ 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.

Algemene opmerkingen

1. Het bij de adviesaanvraag gevoegde dossier bevat geen gedetailleerde uitleg over het verband tussen elk van de bepalingen van het voorontwerp en de bepalingen 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

* Deze verlenging vloeit voort uit artikel 84, § 1, eerste lid, 2°, *in fine*, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, waarin wordt bepaald dat deze termijn van rechtswege verlengd wordt met vijftien dagen wanneer hij begint te lopen tussen 15 juli en 31 juli of wanneer hij verstrijkt tussen 15 juli en 15 augustus.

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

règlement (UE) n° 526/2013" (ci-après: "le règlement sur la cybersécurité") qu'elles tendent à mettre en œuvre.

Dès lors que l'avant-projet a pour objet d'exécuter ce règlement et ne peut être correctement appréhendé que par sa lecture conjointe avec celui-ci, vu également la complexité et la technicité du règlement en question, pareilles explications auraient été utiles à l'instruction et à l'examen de la demande d'avis par la section de législation. Dans ces conditions, en l'absence de pareilles explications, il ne peut être garanti que le Conseil d'État, dans le délai qui lui a été imparti et compte tenu de ce qu'il est soumis actuellement à un nombre très élevé de demandes d'avis, ait pu procéder à un examen exhaustif de l'avant-projet de loi, même si le commentaire de certains articles, mais sans exhaustivité, comporte quelques explications sur la relation entre le règlement et l'avant-projet de loi.

Il est recommandé que pareil document explicatif soit annexé à l'exposé des motifs ou qu'à tout le moins ce dernier, et plus spécialement le commentaire des articles concernés, soit complété par les explications utiles sur ce point.

Par ailleurs, lorsque, comme tel est le cas pour tout règlement et donc aussi pour le règlement sur la cybersécurité, un instrument de droit européen est revêtu de l'effet direct, qui en principe fait obstacle à ce que les règles contenues dans le règlement soient reproduites ou paraphrasées dans le texte national d'exécution, il y a lieu en tout état de cause de compléter celles des dispositions de l'avant-projet qui procèdent de la sorte par la mention selon laquelle elles sont adoptées "conformément à" ces dernières.

en tot intrekking van Verordening (EU) nr. 526/2013" (hierna: "de cyberbeveiligingsverordening") waaraan ze uitvoering beogen te geven.

Aangezien het voorontwerp ertoe strekt uitvoering te geven aan die verordening en enkel correct kan worden begrepen door het in samenhang met die verordening te lezen, mede gelet op de complexiteit en de technische aard van de betrokken verordening, zou een dergelijke uitleg nuttig zijn geweest voor de behandeling en het onderzoek van de adviesaanvraag door de afdeling Wetgeving. In die omstandigheden kan, bij gebrek aan dergelijke toelichtingen, niet worden gewaarborgd dat de Raad van State binnen de hem gestelde termijn en gelet op het feit dat hij thans een zeer groot aantal adviesaanvragen te behandelen heeft, het voorontwerp van wet exhaustief heeft kunnen onderzoeken, ook al bevat de bespreking van bepaalde artikelen, zij het niet uitputtend, enige uitleg over het verband tussen de verordening en het voorontwerp van wet.

Het verdient aanbeveling een dergelijk toelichtende nota bij de memorie van toelichting te voegen of op zijn minst die memorie, en meer in het bijzonder de bespreking van de artikelen in kwestie, aan te vullen met de desbetreffende dienstige uitleg.

Wanneer, zoals het geval is met elke verordening en dus ook met de cyberbeveiligingsverordening, een Europees rechtsinstrument rechtstreeks uitwerking heeft, wat in principe verhindert dat de in de verordening vervatte regels worden overgenomen of geparafraseerd in de nationale uitvoeringstekst, dienen de bepalingen van het voorontwerp die op die wijze zijn geredigeerd, voorts hoe dan ook te worden aangevuld met de vermelding dat ze "overeenkomstig" die Europese regels zijn aangenomen.

La présente observation vaut également pour le lien entre l'avant-projet et d'autres instruments de droit européen[1].

2.1. Plusieurs dispositions de l'avant-projet, notamment les articles 6, §§ 2 à 4, 7, 13, 15, §§ 3, 3° et 4°, 6 et 7, 16, § 2, 17, 37, 39 et 41, concernent ou peuvent impliquer le traitement de données à caractère personnel.

Comme l'a confirmé le fonctionnaire délégué, l'avant-projet n'a pas été soumis à l'Autorité de protection des données.

L'article 36, paragraphe 4, 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"), combiné avec l'article 57, paragraphe 1, c), et le considérant 96 de ce règlement, prévoit une obligation de consulter l'autorité de contrôle, à savoir l'Autorité de protection des données créée par 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 qui se rapporte au traitement de données à caractère personnel.

Il convient dès lors de veiller à l'accomplissement de cette formalité.

2.2. Il convient toutefois d'attirer déjà l'attention de l'auteur de l'avant-projet sur les principes fondamentaux régissant

[1] Ainsi, par exemple, le règlement sur la cybersécurité fait systématiquement référence à la directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 "concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union". Le considérant n° 15 du préambule au règlement sur la cybersécurité se réfère à cette directive et énonce également que "[d]'autres actes juridiques tels que 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)"] et les directives 2002/58/CE ['concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques'] et (UE) 2018/1972 ['établissant le code des communications électroniques européen'] contribuent également à un niveau élevé de cybersécurité dans le marché unique numérique". Les explications relatives aux relations entre le projet de loi et son cadre européen gagneront, s'il y a lieu, à faire état de ces textes, étant entendu que, lorsqu'il s'agit des directives, leurs textes nationaux de transposition seront également renseignés: s'agissant par exemple de la directive 2016/1148, il s'agit 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 12 juillet 2019 "portant exécution 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, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques".

Deze opmerking geldt eveneens voor het verband tussen het voorontwerp en andere instrumenten van Europees recht.[1]

2.1. Een aantal bepalingen van het voorontwerp, met name de artikelen 6, §§ 2 tot 4, 7, 13, 15, §§ 3, 3° en 4°, 6 en 7, 16, § 2, 17, 37, 39 en 41, hebben betrekking op, of impliceren mogelijk, de verwerking van persoonsgegevens.

Zoals de gemachtigde ambtenaar heeft bevestigd, is het voorontwerp niet voorgelegd aan de Gegevensbeschermingsautoriteit.

Artikel 36, lid 4, 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"), gelezen in samenhang met artikel 57, lid 1, c), en overweging 96 van die verordening, voorziet in een verplichting om de toezichthoudende autoriteit, namelijk de Gegevensbeschermingsautoriteit opgericht bij de wet van 3 december 2017 "tot oprichting van de Gegevensbeschermingsautoriteit", te raadplegen bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel in verband met de verwerking van persoonsgegevens.

Er moet dus voor gezorgd worden dat dat vormvereiste wordt vervuld.

2.2. De aandacht van de steller van het voorontwerp dient echter reeds te worden gevestigd op de grondbeginselen die

[1] Zo bijvoorbeeld verwijst de cyberbeveiligingsverordening systematisch naar richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 "betreffende maatregelen om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie te waarborgen". Overweging 15 van de aanhef van de cyberbeveiligingsverordening verwijst naar die richtlijn en bepaalt ook dat "[a]ndere rechtshandelingen zoals 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)"] en de richtlijnen 2002/58/EG ['betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie'] en (EU) 2018/1972 ['tot vaststelling van het Europees wetboek voor elektronische communicatie'] (…) eveneens [bijdragen] tot een hoog niveau van cyberbeveiliging in de digitale eengemaakte markt". De uitleg over het verband tussen het wetsontwerp en zijn Europese kader zou, waar nodig, die teksten moeten vermelden, met dien verstande dat, wanneer het gaat om richtlijnen, hun nationale omzettingsteksten eveneens moeten worden vermeld: wat bijvoorbeeld richtlijn 2016/1148 betreft, gaat het om 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 om het koninklijk besluit van 12 juli 2019 "tot uitvoering 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 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren".

les traitements des données personnelles envisagés par le texte à l'examen.

2.3. Dans son avis 68.936/AG donné le 7 avril 2021 sur l'avant-projet devenu la loi du 14 août 2021 "relative aux mesures de police administrative lors d'une situation d'urgence épidémique", l'assemblée générale de la section de législation a exposé ce qui suit:

"101. Conformément à l'article 22 de la Constitution, tout traitement de données à caractère personnel et, plus généralement, toute atteinte au droit à la vie privée, sont soumis au respect d'un principe de légalité formelle […].

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 ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les "éléments essentiels" sont fixés préalablement par le législateur[2].

Par conséquent, les "éléments essentiels" des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, la section de législation considère que, quelle que soit la matière concernée, constituent, en principe, des "éléments essentiels" les éléments suivants: 1°) les catégories de données traitées; 2°) les catégories de personnes concernées; 3°) la finalité poursuivie par le traitement; 4°) les catégories de personnes ayant accès aux données traitées; et 5°) le délai maximal de conservation des données.

[…]

104. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement se fonder sur une disposition législative suffisamment précise (principe de légalité matérielle), mais aussi reposer sur une justification objective et raisonnable et, par conséquent, être proportionnée aux buts poursuivis par le législateur, qui dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée: pour qu'une norme soit compatible avec le droit au

[2] *Note de bas de page n° 175 de l'avis cité:* Jurisprudence constante de la Cour constitutionnelle: voir notamment C.C., 18 mars 2010, n° 29/2010, B.16.1; C.C., 20 février 2020, n° 27/2020, B.17.

gelden voor de verwerkingen van persoonsgegevens die de voorliggende tekst in het vooruitzicht stelt.

2.3. In haar advies 68.936/AV van 7 april 2021 over het voorontwerp dat heeft geleid tot de wet van 14 augustus 2021 "betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie" heeft de algemene vergadering van de afdeling Wetgeving het volgende uiteengezet:

"101. Krachtens artikel 22 van de Grondwet geldt voor elke verwerking van persoonsgegevens en, meer in het algemeen, voor elke schending van het recht op het privéleven, dat het formeel legaliteitsbeginsel dient te worden nageleefd (…).

Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de "essentiële elementen" voorafgaandelijk door de wetgever vastgesteld zijn.[2]

Bijgevolg moeten de "essentiële elementen" van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd. In dat verband is de afdeling Wetgeving van oordeel dat ongeacht de aard van de betrokken aangelegenheid, de volgende elementen in beginsel "essentiële elementen" uitmaken: 1°) de categorie van verwerkte gegevens; 2°) de categorie van betrokken personen; 3°) de met de verwerking nagestreefde doelstelling; 4°) de categorie van personen die toegang hebben tot de verwerkte gegevens; en 5°) de maximumtermijn voor het bewaren van de gegevens.

(…)

104. Overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling (materieel legaliteitsbeginsel), ze dient daarenboven op een objectieve en redelijke verantwoording te berusten en bijgevolg evenredig te zijn met de doelstellingen die nagestreefd worden door de wetgever, die ter zake over enige beoordelingsruimte beschikt. Die beoordelingsruimte is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk

[2] *Voetnoot 175 van het geciteerde advies:* Vaste rechtspraak van het Grondwettelijk Hof: zie inzonderheid GwH 18 maart 2010, nr. 29/2010, B.16.1; GwH 20 februari 2020, nr. 27/2020, B.17.

respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause[3]"[4].

L'article 7 de la Charte des droits fondamentaux de l'Union européenne, qui garantit notamment le droit au respect de la vie privée, ainsi que l'article 8, paragraphe 1, de la même Charte et l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne, lesquels disposent que toute personne a droit à la protection des données à caractère personnel la concernant, ont été mis en œuvre par le RGPD, dont le chapitre II énonce les principes applicables aux traitements de données à caractère personnel.

Parmi ces principes, l'article 5 du RGPD énonce, en les développant, ceux relatifs à la licéité, à la loyauté et à la transparence, à la limitation des finalités, à la minimisation des données, à l'exactitude, à la limitation de la conservation, à l'intégrité et à la confidentialité, ainsi qu'à la responsabilité.

S'agissant de la licéité du traitement, l'article 6, paragraphes 1, c) et e), et 3, du RGPD énonce ce qui suit:

"1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

[…]

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

[…]

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

[…]

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par:

a) le droit de l'Union; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn.[3]"[4]

Artikel 7 van het Handvest van de grondrechten van de Europese Unie, dat onder meer het recht op eerbiediging van het privéleven waarborgt, alsook artikel 8, lid 1, van hetzelfde Handvest en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie, die bepalen dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens, zijn ten uitvoer gelegd bij de AVG, waarvan hoofdstuk II de beginselen formuleert die van toepassing zijn op de verwerkingen van persoonsgegevens.

Van die beginselen worden in artikel 5 van de AVG de volgende vermeld en uiteengezet: de beginselen van rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, alsook verantwoordingsplicht.

Met betrekking tot de rechtmatigheid van de verwerking bepaalt artikel 6, lid 1, c) en e), en lid 3, van de AVG het volgende:

"1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

(…)

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

(…)

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

(…)

3. De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij:

a) Unierecht; of

b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

---

3 *Note de bas de page n° 185 de l'avis cité:* Avis C.E. n° 63.202/2 donné le 26 avril 2018 sur un avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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 (*Doc. [p]arl.*, Chambre, sess. 2017-2018, n° 54-3185/001, p. 121-122).

4 Avis 68.936/AG donné le 7 avril 2021 sur l'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. 119, 121 et 122).

3 *Voetnoot 185 van het geciteerde advies*: Advies RvS 63.202/2 van 26 april 2018 over een voorontwerp van wet "tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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" (*Parl.St.* Kamer 2017-18, nr. 54-3185/001, 121-122).

4 Advies 68.936/AV van 7 april 2021 over een voorontwerp dat heeft geleid 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, 119, 121 en 122).

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi".

Ces principes font écho à ceux qui résultent de la légisprudence de la section de législation, tels qu'ils ont été synthétisés dans l'avis 68.936/AG précité du 7 avril 2021 et rappelés ci-avant.

2.4. L'avant-projet de loi est lacunaire sur de nombreux aspects touchant aux exigences ainsi résumées, s'agissant spécialement de l'identification expresse des finalités poursuivies, des catégories de données et de personnes concernées, des catégories de destinataires des données et du délai maximal de conservation des données.

Il appartient à l'auteur de l'avant-projet de le compléter substantiellement sur ces points conformément à l'article 22 de la Constitution, à l'article 8 de la Convention européenne des droits de l'homme et au RGPD.

À cet égard, l'indication figurant aux paragraphes 3 et 4 de l'article 6 de l'avant-projet, aux termes de laquelle les échanges d'information prévues par ces dispositions "se limitent à ce qui est pertinent et proportionné à l'objectif de cet échange, notamment dans le respect du [RGPD]", ne saurait satisfaire aux obligations tirées du règlement européen, lesquelles impliquent des dispositifs propres au cadre juridique envisagé par la loi en projet et à son champ d'application. Il convient en outre de rappeler qu'un règlement européen a un effet direct et qu'il n'y a pas lieu d'en rappeler l'applicabilité. Il convient au contraire, lorsque, comme en l'espèce, le règlement prescrit un certain nombre d'obligations pesant sur les autorités nationales, en premier lieu aux législateurs, que ces obligations soient expressément mises en œuvre.

2.5. Il résulte de l'effet direct du RGPD que son chapitre III ("Droits de la personne concernée") et ses articles 12 à 22 s'appliquent de plein droit.

Compte tenu de l'objet de la législation en projet, la question se pose toutefois s'il n'y a pas lieu pour l'auteur de l'avant-projet d'envisager l'application de l'article 23, paragraphe 1, du RGPD,

Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel".

Die beginselen sluiten aan bij de beginselen die voortvloeien uit de adviespraktijk van de afdeling Wetgeving, zoals ze zijn gesynthetiseerd in het voornoemde advies 68.936/AV van 7 april 2021 en hierboven zijn aangehaald.

2.4. Het voorontwerp van wet vertoont lacunes op tal van punten die betrekking hebben op de aldus samengevatte vereisten, met name wat betreft het uitdrukkelijk aangeven van de nagestreefde doelen, de categorieën van gegevens en van betrokkenen, de categorieën van ontvangers van de gegevens en de maximale opslagperiode van de gegevens.

Het staat aan de steller van het voorontwerp om het voorontwerp op die punten substantieel aan te vullen overeenkomstig artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de AVG.

In dat verband kan de in de paragrafen 3 en 4 van artikel 6 van het voorontwerp opgenomen vermelding, luidens welke de in die bepalingen bedoelde uitwisseling van informatie "wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van deze uitwisseling, met name overeenkomstig de [AVG]", niet voldoen aan de verplichtingen die voortvloeien uit de Europese verordening; die verplichtingen impliceren teksten die geëigend zijn voor het bij de ontworpen wet beoogde juridische kader en de werkingssfeer ervan. Bovendien dient te worden opgemerkt dat een Europese verordening rechtstreeks uitwerking heeft het niet aanvaardbaar is de toepasselijkheid ervan in herinnering te brengen. Wanneer de verordening, zoals in dit geval, een aantal verplichtingen oplegt aan de nationale autoriteiten, in de eerste plaats aan de wetgevers, moet daarentegen uitdrukkelijk uitvoering worden gegeven aan die verplichtingen.

2.5. Uit de rechtstreekse uitwerking van de AVG volgt dat hoofdstuk III ("Rechten van de betrokkene") en de artikelen 12 tot 22 van die verordening van rechtswege van toepassing zijn.

Gelet op het voorwerp van de ontworpen wetgeving rijst echter de vraag of de steller van het voorontwerp niet moet overwegen toepassing te maken van artikel 23, lid 1, van

dont il résulte que la loi peut “limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l’article 34, ainsi qu’à l’article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu’une telle limitation respecte l’essence des libertés et droits fondamentaux et qu’elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir” divers objectifs énumérés aux litteras a) à j) de cet article 23, paragraphe 1, et à la condition que la “mesure législative visée au paragraphe 1 contien[ne] des dispositions spécifiques relatives, au moins, le cas échéant”, à divers objets énumérés au paragraphe 2 de cet article 23.

2.6. L’avant-projet de loi doit être fondamentalement revu à la lumière de ces observations et son exposé des motifs contiendra les explications utiles à ce sujet.

Observations particulières

Articles 2 et 4

Compte tenu du contenu de l’article 3, § 1er, de l’avant-projet, mieux vaut omettre le 1° de l’article 4 et insérer les mots “, ci-après: le “règlement sur la cybersécurité”” dans l’article 2, *in fine*, de l’avant-projet.

Article 3

1. Au paragraphe 4, il convient de remplacer les mots “l’article 6, § 1er, de la loi du 7 avril 2019” par les mots “l’article 6, 2°, de la loi du 7 avril 2019”.

2. La portée du paragraphe 3 est obscure. Si sa seule vocation est de faire écho à l’article 1, paragraphe 2, du règlement sur la cybersécurité, alors il n’a pas sa place dans l’avant-projet dès lors que la disposition précitée a elle-même pour seule portée de rappeler la compétence des États membres “en ce qui concerne les activités relatives à la sécurité publique, à la défense et à la sécurité nationale, et les activités de l’État dans des domaines du droit pénal”. Si le texte devait avoir une autre portée, elle sera clarifiée dans l’exposé des motifs.

3. De l’accord du fonctionnaire délégué, l’article 3 de l’avant-projet sera complété par la disposition suivante:

“§ 6. 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”.

de AVG, waaruit voortvloeit dat de wet “[de] reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 voor zover de bepalingen van dat artikel overeenkomen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 22, [kan beperken] op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van” diverse doelstellingen opgesomd in de *litterae* a) tot j) van dat artikel 23, lid 1, en op voorwaarde dat “de in lid 1 bedoelde wettelijke maatregelen (…) met name specifieke bepalingen [bevatten] met betrekking tot, in voorkomend geval, ten minste” verscheidene in lid 2 van dat artikel 23 genoemde doeleinden.

2.6. Het voorontwerp van wet moet in het licht van die opmerkingen grondig worden herzien en de memorie van toelichting moet de uitleg bevatten die in dat verband nuttig is.

Bijzondere opmerkingen

Artikelen 2 en 4

Gelet op de inhoud van artikel 3, § 1, van het voorontwerp, zou het beter zijn om punt 1° weg te laten uit artikel 4 en om de woorden “, hierna: de “cyberbeveiligingsverordening”” in te voegen op het einde van artikel 2 van het voorontwerp.

Artikel 3

1. In paragraaf 4 dienen de woorden “artikel 6, § 1, van de wet van 7 april 2019” te worden vervangen door de woorden “artikel 6, 2°, van de wet van 7 april 2019”.

2. De strekking van paragraaf 3 is onduidelijk. Als de enige bedoeling van die paragraaf erin bestaat artikel 1, lid 2, van de cyberbeveiligingsverordening weer te geven, dan hoort hij niet thuis in het voorontwerp, aangezien de voormelde bepaling er op haar beurt enkel toe strekt te wijzen op de bevoegdheid van de lidstaten “betreffende activiteiten op het gebied van openbare veiligheid, defensie, nationale veiligheid en activiteiten van de staat op het gebied van het strafrecht”. Indien de tekst een andere strekking zou hebben, moet die worden verduidelijkt in de memorie van toelichting.

3. De gemachtigde ambtenaar is het ermee eens dat artikel 3 van het voorontwerp met de volgende bepaling moet worden aangevuld:

“§ 6. 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.”

Article 5

Aux paragraphes 2, alinéa 1er, et 3, il convient de remplacer les mots “à l’article 5, § 1er” par les mots “au paragraphe 1er”.

Article 12

Le fonctionnaire délégué a proposé que l’article 12 soit remplacé par le texte suivant:

“En cas de refus de délivrance d’un certificat de cybersécurité européen par l’autorité visée à l’article 5, § 1er, ou par un organisme d’évaluation de la conformité dans le cadre de la délégation prévue à l’article 10, § 3, ou à l’article 11, § 2, le demandeur peut introduire une réclamation devant l’autorité visée à l’article 5, § 1er, selon les modalités prévues au chapitre 7”.

La proposition du fonctionnaire délégué peut être suivie.

Article 13

Le fonctionnaire délégué a proposé que l’alinéa 1er du paragraphe 1er soit remplacé par le texte suivant:

“L’autorité visée à l’article 5, § 1er, dispose d’un service d’inspection qui, sans préjudice de l’application de l’arrêté royal du 31 janvier 2006 portant création du système BELAC d’accréditation des organismes d’évaluation de la conformité, peut à tout moment réaliser des contrôles du respect par les organismes d’évaluation de la conformité, les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l’Union européenne des règles imposées par le règlement sur la cybersécurité, les schémas européens de certification de cybersécurité, la présente loi ou ses arrêtés d’exécution”.

La proposition du fonctionnaire délégué peut être suivie.

Article 23

1. L’article 23, § 1er, énonce que

“[t]oute infraction au Règlement sur la cybersécurité, ainsi qu’à la loi en projet ou ses arrêtés d’exécution peut faire l’objet d’une sanction administrative”.

Il n’apparaît pas clairement si la liste des infractions administratives prévues spécifiquement aux paragraphes suivants de la même disposition épuise de manière exhaustive la gamme des comportements qui seront pareillement sanctionnables sur la base du paragraphe 1er ou s’il ne s’agit là que d’une liste

Artikel 5

In de paragrafen 2, eerste lid, en 3 dienen de woorden “in artikel 5, § 1” te worden vervangen door de woorden “in paragraaf 1”.

Artikel 12

De gemachtigde ambtenaar heeft voorgesteld artikel 12 te vervangen door de volgende tekst:

“Ingeval de afgifte van een Europees cyberbeveiligingscertificaat geweigerd wordt door de in artikel 5, § 1, bedoelde autoriteit of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie waarin artikel 10, § 3, of artikel 11, § 2, voorziet, kan de aanvrager een klacht indienen bij de autoriteit bedoeld in artikel 5, § 1, volgens de in hoofdstuk 7 bepaalde modaliteiten.”

Het voorstel van de gemachtigde ambtenaar kan worden gevolgd.

Artikel 13

De gemachtigde ambtenaar heeft voorgesteld het eerste lid van paragraaf 1 te vervangen door de volgende tekst:

“De autoriteit bedoeld in artikel 5, § I, beschikt over een inspectiedienst die, onverminderd de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling, op elk ogenblik controles kan uitvoeren om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de cyberbeveiligingsverordening, de Europese cyberbeveiligingscertificeringsregelingen, deze wet of de uitvoeringsbesluiten ervan.”

Het voorstel van de gemachtigde ambtenaar kan worden gevolgd.

Artikel 23

1. Artikel 23, § 1, luidt als volgt:

“Elke inbreuk op de Cyberbeveiligingsverordening, op deze wet of op de uitvoeringsbesluiten ervan kan aanleiding geven tot een administratieve sanctie.”

Het is niet duidelijk of de lijst van de administratieve overtredingen die specifiek worden bepaald in de volgende paragrafen van dezelfde bepaling, een exhaustieve opsomming is van alle gedragingen die op basis van paragraaf 1 op dezelfde wijze strafbaar worden, dan wel of het hier slechts

exemplative, en sorte que d'autres comportements que ceux y visés pourront valoir à leur auteur une sanction administrative.

Dans la première hypothèse, le paragraphe 1er serait inutile et devrait être omis pour éviter toute ambiguïté. Dans la seconde, le dispositif en projet devrait être complété pour prévoir[5] les montants minimum et maximum des amendes administratives susceptibles de sanctionner les comportements "autres" que ceux qui sont spécifiquement visés par les paragraphes 2 et suivants.

2. Le paragraphe 6 punit d'une amende administrative de 500 à 150 000 euros quiconque ne coopère pas lors d'un contrôle, par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle.

Comme la section de législation l'a rappelé à diverses reprises,

"[l]e droit de ne pas s'auto-incriminer, garanti par l'article 6 de la Convention européenne des droits de l'homme, fait toutefois obstacle à ce qu'une personne, "pénalement accusée" au sens de cette disposition, puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité"[6].

L'article 15, § 5, alinéa 1er, 3°, de l'avant-projet prévoit au demeurant que la personne auditionnée par le service de l'inspection a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Partant, et pour toute clarté, il y a lieu d'ajouter au début du paragraphe 6 les mots "Sans préjudice de l'article 15, § 5, alinéa 1er, 3°,".

3. En outre, compte tenu de ce qu'il convient d'éviter d'insérer des éléments exemplatifs dans un dispositif normatif, au paragraphe 6, les mots ", par exemple en refusant de communiquer

een voorbeeldlijst betreft, zodat ook andere dan de daarin vermelde gedragingen tot een administratieve sanctie kunnen leiden voor de persoon in kwestie.

In het eerste geval zou paragraaf 1 nutteloos zijn en zou hij moeten worden weggelaten teneinde verwarring te voorkomen. In het tweede geval zou het ontworpen dispositief aanvullend het minimum- en het maximumbedrag moeten bepalen[5] van de administratieve geldboeten waarmee "andere" gedragingen kunnen worden bestraft dan die welke specifiek in de paragrafen 2 en volgende worden bedoeld.

2. Paragraaf 6 bepaalt dat eenieder die weigert mee te werken tijdens een inspectie, bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken, met een geldboete van 500 tot 150 000 euro wordt gestraft.

De afdeling Wetgeving heeft er reeds herhaaldelijk op gewezen dat

"het recht om zichzelf niet te beschuldigen, dat gewaarborgd is door artikel 6 van het Europees Verdrag voor de rechten van de mens, staat er evenwel aan in de weg dat een persoon, "tegen wie een vervolging is ingesteld", in de zin van die bepaling, kan worden bestraft omdat hij geweigerd heeft zijn medewerking te verlenen bij het bewijzen van zijn eigen schuld".[6]

Artikel 15, § 5, eerste lid, 3°, van het voorontwerp bepaalt voorts dat de persoon die door de inspectiedienst wordt verhoord, het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

Voor alle duidelijkheid moeten de woorden "Onverminderd artikel 15, § 5, eerste lid, 3°," dan ook aan het begin van paragraaf 6 worden toegevoegd.

3. Gelet op het feit dat men dient te vermijden in een normatieve tekst voorbeelden op te nemen, moeten in paragraaf 6 bovendien de woorden ", bijvoorbeeld door te weigeren de

---

5 Avis 54.983/2/VR donné le 18 février 2014 sur un avant-projet devenu la loi du 25 avril 2014 "visant à insérer un article 36/45 à la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique" (*Doc. parl.*, Chambre, 2013-2014, n° 3414/1, pp. 43 à 52; *http://www.raadvst-consetat.be/dbx/avis/54983.pdf*).

6 Avis 60.619/2 donné le 25 janvier 2017 sur un avant-projet devenu la loi du 2 octobre 2017 "réglementant la sécurité privée et particulière" (*Doc. parl.*, Chambre, 2016-2017, n° 2388/1, p. 194; *http://www.raadvst-consetat.be/dbx/avis/60619.pdf*). Voir aussi les avis 63.296/4 donné le 2 mai 2018 sur un avant-projet devenu 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" (*Doc. parl.*, Chambre, 2018-2019, n° 3340/1, pp. 75 à 87; *http://www.raadvst-consetat.be/dbx/avis/63296.pdf*) et 64.879/4 donné le 4 février 2019 sur un avant-projet devenu le décret du 2 mai 2019 "modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé" (*Doc. parl.*, Parl. wall., 2018-2019, n° 1332/1, pp. 25 à 35; *http://www.raadvst-consetat.be/dbx/avis/64879.pdf*).

5 Advies 54.983/2/VR, op 18 februari 2014 gegeven over een voorontwerp dat heeft geleid tot de wet van 25 april 2014 "tot invoeging van een artikel 36/45 in de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België" (*Parl.St.* Kamer 2013-14, nr. 3414/001, 43-52; *http://www.raadvst-consetat.be/dbx/adviezen/54983.pdf).*

6 Advies 60.619/2, op 25 januari 2017 gegeven over een voorontwerp dat heeft geleid tot de wet van 2 oktober 2017 "tot regeling van de private en bijzondere veiligheid" (*Parl.St.* Kamer 2016-17, nr. 2388/001, 194; *http://www.raadvst-consetat.be/dbx/adviezen/60619.pdf*). Zie ook de adviezen 63.296/4, op 2 mei 2018 gegeven over een voorontwerp dat heeft geleid tot 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" (*Parl.St*. Kamer 2018-19, nr. 3340/001, 75-87; *http://www.raadvst-consetat.be/dbx/adviezen/63296.pdf*) en 64.879/4, op 4 februari 2019 gegeven over een voorontwerp dat heeft geleid tot het decreet van 2 mei 2019 "tot wijziging van het Waalse Wetboek van Sociale Actie en Gezondheid wat betreft de preventie en de bevordering van de gezondheid" (*Parl.St.* W.Parl. 2018-19, nr. 1332/1, 25-35; *http://www.raadvst-consetat.be/dbx/adviezen/64879.pdf*).

les informations qui lui sont demandées à l'occasion de ce contrôle" seront remplacés par les mots "en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou de toute autre manière".

Le commentaire des articles pourra par ailleurs être complété sur ce point.

Articles 24 et 33

L'obligation de motivation formelle, prévue aux articles 24, § 1er, première phrase, et 33, alinéa 2, *in fine*, résulte déjà de la loi du 29 juillet 1991 "relative à la motivation formelle des actes administratifs".

Elle ne doit dès lors pas être réitérée dans l'avant-projet.

Article 26

L'alinéa 5 prévoit que le recours introduit auprès de la Cour des marchés visée à l'article 101 du Code judiciaire ne suspend pas la décision prise en vertu du chapitre 6 par l'autorité visée à l'article 5, § 1er.

Compte tenu des lourdes conséquences que l'absence d'effet suspensif de la décision peut avoir sur la situation du contrevenant et de ce que, dans d'autres circonstances pouvant être comparables, un effet suspensif est accordé aux recours introduits, il y a lieu à tout le moins de préciser dans l'exposé des motifs, et compte tenu du juste équilibre à réaliser entre les intérêts en présence[7], les raisons pour lesquelles en l'espèce l'absence d'effet du recours suspensif doit être imposé[8].

Article 29

Le fonctionnaire délégué a proposé que l'alinéa 1er du paragraphe 1er soit remplacé par le texte suivant:

"L'autorité visée à l'article 5, § 1er, reçoit et traite les réclamations des personnes en rapport avec un certificat de cybersécurité européen délivré par l'autorité visée à l'article 5,

7 Voir en effet Cour eur. D.H., arrêt *Janosevic c. Suède*, 23 juillet 2002, §§ 105 et 106; Trib. UE, 27 mars 2014, *Saint Gobain Glass France S.A. c. Commission,* § 104: "En tout état de cause, il y a lieu de relever que la Cour européenne des droits de l'homme, dans son arrêt Janosevic c. Suède, du 23 juillet 2002 (*Recueil des arrêts et décisions,* 2002-VII, p. 1, § 106 à 110), a jugé que le droit à la présomption d'innocence ne s'opposait pas, en principe, à ce que des sanctions de nature pénale adoptées par un organe administratif puissent être mises à exécution avant qu'elles soient devenues définitives, au terme d'une procédure de recours devant un tribunal, pourvu qu'une telle exécution s'inscrive dans des limites raisonnables ménageant un juste équilibre entre les intérêts en jeu et que le destinataire de la sanction puisse être rétabli dans sa situation initiale en cas de succès de son recours".

8 En ce sens: C.C., 30 juin 2011, n° 119/2011.

naar aanleiding van deze inspectie gevraagde informatie te verstrekken" worden vervangen door de woorden "door te weigeren de naar aanleiding van deze inspectie of anderszins gevraagde informatie te verstrekken".

De artikelsgewijze bespreking kan op dat punt nog worden aangevuld.

Artikelen 24 en 33

De verplichting tot uitdrukkelijke motivering waarin de artikelen 24, § 1, eerste zin, en 33, tweede lid, *in fine*, voorzien, vloeit reeds voort uit de wet van 29 juli 1991 "betreffende de uitdrukkelijke motivering van de bestuurshandelingen".

Ze moet dan ook niet worden herhaald in het voorontwerp.

Artikel 26

In het vijfde lid wordt bepaald dat het beroep ingesteld bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek, de beslissing die de in artikel 5, § 1, bedoelde overheid krachtens hoofdstuk 6 genomen heeft, niet schorst.

Gelet op de verregaande gevolgen die het ontbreken van de schorsende werking van de beslissing kan hebben op de situatie van de overtreder, en gelet op het feit dat in andere mogelijk vergelijkbare omstandigheden schorsende werking verleend wordt aan de ingestelde beroepen, moet men in de memorie van toelichting op zijn minst preciseren, tevens gelet op het billijke evenwicht dat tussen de in het geding zijnde belangen tot stand moet worden gebracht,[7] waarom *in casu* moet worden voorgeschreven dat het beroep geen schorsende werking heeft.[8]

Artikel 29

De gemachtigde ambtenaar heeft voorgesteld het eerste lid van paragraaf 1 te vervangen door de volgende tekst:

"De autoriteit bedoeld in artikel 5, § l, ontvangt en behandelt klachten van personen over een Europees cyberbeveiligingscertificaat afgegeven door de in artikel 5, § 1, bedoelde

7 Zie immers EHRM 23 juli 2002, arrest *Janosevic t. Zweden*, §§ 105 en 106; Ger.EU 27 maart 2014, *Saint-Gobain Glass France S.A. t. Commissie,* § 104: "Hoe dan ook moet worden opgemerkt dat het Europees Hof voor de Rechten van de Mens in zijn arrest Janosevic v. Zweden van 23 juli 2002 (*Recueil des arrêts et décisions*, 2002-VII, blz. 1, § 106-110) heeft geoordeeld dat het recht op de onschuldpresumptie zich in beginsel niet ertegen verzet dat door een administratief orgaan vastgestelde sancties van strafrechtelijke aard ten uitvoer kunnen worden gelegd voordat zij na een beroepsprocedure voor een rechterlijke instantie definitief zijn geworden, mits een dergelijke tenuitvoerlegging wordt toegepast binnen redelijke grenzen die een redelijk evenwicht tussen de betrokken belangen tot stand brengen, en de oorspronkelijke situatie van degene aan wie de sanctie wordt opgelegd, kan worden hersteld indien diens beroep slaagt."

8 In die zin: GwH 30 juni 2011, nr. 119/2011.

§ 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation prévue à l'article 10, § 3, ou 11, § 2, avec le refus de délivrance d'un tel certificat ou avec une déclaration de conformité de l'Union européenne".

La proposition du fonctionnaire délégué peut être suivie.

Article 34

Il convient de remplacer les mots "articles 11, 12, 21 et 22" par les mots "articles 10, 11, 21 et 22".

Article 35

À l'alinéa 1er, il convient de remplacer les mots "du chapitre 7" par les mots "de la section 1re".

Articles 40 et 41

Les articles 40 et 41 seront intervertis.

Chapitre 8

Les sections 1ère à 4 du chapitre 8 contiennent des dispositions modificatives de diverses lois et non des dispositions finales.

L'intitulé du chapitre 8 sera donc remplacé par le suivant: "Dispositions modificatives".

La section 5 formera en conséquence un chapitre 9 nouveau. Dès lors qu'il ne contient pas de disposition transitoire, les mots "et dispositions transitoires" seront en conséquence omis de son intitulé.

Articles 45 et 47

Dans l'article XV.30/3 en projet du Code de droit économique (article 45 de l'avant-projet), il est précisé que le Roi peut confier certaines missions relatives à la certification de cybersécurité à la demande du SPF Économie à certains agents de ce SPF.

Contrairement à la Banque nationale de Belgique et à l'Autorité des services et marchés financiers (FSMA), lesquelles ont une personnalité juridique distincte de l'État fédéral, le SPF Économie fait partie des services de l'administration générale.

En vertu des articles 37 et 107, alinéa 2, de la Constitution, il revient au Roi de régler l'organisation des services publics

autoriteit of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie waarin artikel 10, § 3, of artikel 11, § 2, voorziet, over de weigering om een dergelijk certificaat af te geven of over een EU-conformiteitsverklaring."

Het voorstel van de gemachtigde ambtenaar kan worden gevolgd.

Artikel 34

De woorden "artikelen 11, 12, 21 en 22" dienen te worden vervangen door de woorden "artikelen 10, 11, 21 en 22".

Artikel 35

In het eerste lid dienen de woorden "hoofdstuk 7" te worden vervangen door de woorden "afdeling 1".

Artikelen 40 en 41

De artikelen 40 en 41 moeten onderling van plaats worden verwisseld.

Hoofdstuk 8

De afdelingen 1 tot 4 van hoofdstuk 8 bevatten bepalingen tot wijziging van verschillende wetten, en geen slotbepalingen.

Het opschrift van hoofdstuk 8 moet dus worden vervangen door het opschrift "Wijzigingsbepalingen".

Als gevolg daarvan moet afdeling 5 een nieuw hoofdstuk 9 vormen. Aangezien dat hoofdstuk geen overgangsbepalingen bevat, moeten de woorden "en overgangsbepalingen" dan ook uit het opschrift ervan worden weggelaten.

Artikelen 45 en 47

In het ontworpen artikel XV.30/3 van het Wetboek van economisch recht (artikel 45 van het voorontwerp) wordt gepreciseerd dat de Koning op verzoek van de FOD Economie bepaalde opdrachten inzake de certificering van de cyberbeveiliging kan toevertrouwen aan bepaalde ambtenaren van de FOD Economie.

In tegenstelling tot de Nationale Bank van België en de Autoriteit voor Financiële Diensten en Markten (FSMA), die een eigen rechtspersoonlijkheid hebben die losstaat van de Federale Staat, maakt de FOD Economie deel uit van de diensten van het algemeen bestuur.

Krachtens de artikelen 37 en 107, tweede lid, van de Grondwet, staat het aan de Koning om de organisatie van

fédéraux. Il en résulte que le législateur doit s'abstenir de s'y immiscer[9].

Par conséquent, les mots ", à la demande du SPF Économie" (première phrase de l'article XV.30/3 en projet) ainsi que les mots "et avec le SPF Économie" (deuxième phrase de cet article) doivent être omis.

La même observation vaut pour l'article XV.30/4, § 1er, en projet du Code de droit économique (article 47 de l'avant-projet).

Article 47

De l'accord du fonctionnaire délégué, dans la phrase liminaire de l'article 47, les mots "Par dérogation au paragraphe 2 de l'article 3 de la présente loi, il est inséré dans la sous-section 2, inséré par l'article 46, un article XV.30/4" seront remplacés par les mots "Dans la sous-section 2, insérée par l'article 46, il est inséré un article XV.30/4".

Articles 48 et 49

Actuellement, le livre XV, titre 3, chapitre 2, section 11/3, du Code de droit économique ne contient que les articles XV.125/3 et XV.125/4.

Selon le fonctionnaire délégué, un avant-projet de loi "portant des dispositions diverses en matière d'économie", lequel n'a pas encore été soumis à la section de législation, tend à insérer les nouveaux articles XV.125/5 et XV.125/6 dans cette section du Code.

Il conviendra, le cas échéant, d'adapter la numérotation des articles XV.125/7 et XV.125/8 en projet.

[9] Voir notamment l'avis 37.904/4 donné le 22 décembre 2004 sur une proposition de loi "visant à créer un SPF Migrations, à supprimer l'Office des étrangers et à transférer les missions de politique des étrangers et d'asile du SPF Intérieur au SPF Migrations" (*Doc. parl.*, Chambre, 2004-2005, n° 51-1465/2; *http://www.raadvst-consetat.be/dbx/avis/37904.pdf*).

de federale overheidsdiensten te regelen. Daaruit volgt dat de wetgever zich daarin niet heeft te mengen.[9]

Bijgevolg moeten de woorden ", op verzoek van de FOD Economie" (eerste zin van het ontworpen artikel XV.30/3) en de woorden "en de FOD Economie" (tweede zin van dat artikel) worden weggelaten.

Dezelfde opmerking geldt voor het ontworpen artikel XV.30/4, § 1, van het Wetboek van economisch recht (artikel 47 van het voorontwerp).

Artikel 47

De gemachtigde ambtenaar is het ermee eens dat in de inleidende zin van artikel 47 de woorden "In afwijking van paragraaf 2 van artikel 3 van deze wet, wordt in onderafdeling 2, ingevoegd bij artikel 46, een artikel XV.30/4 ingevoegd" moeten worden vervangen door de woorden "In onderafdeling 2, ingevoegd bij artikel 46, wordt een artikel XV.30/4 ingevoegd".

Artikelen 48 en 49

Boek XV, titel 3, hoofdstuk 2, afdeling 11/3, van het Wetboek van economisch recht bevat thans enkel de artikelen XV.125/3 en XV.125/4.

Volgens de gemachtigde ambtenaar strekt een nog niet aan de afdeling Wetgeving voorgelegd voorontwerp van wet "houdende diverse bepalingen inzake economie" ertoe de nieuwe artikelen XV.125/5 en XV.125/6 in te voegen in die afdeling van het wetboek.

De nummering van de ontworpen artikelen XV.125/7 en XV.125/8 dient in voorkomend geval te worden aangepast.

[9] Zie inzonderheid advies 37.904/4, op 22 december 2004 gegeven over een wetsvoorstel "tot oprichting van een FOD Migratie, tot afschaffing van de Dienst Vreemdelingenzaken en tot overheveling van de taken inzake het vreemdelingen- en het asielbeleid van de FOD Binnenlandse Zaken naar de FOD Migratie" (*Parl.St.* Kamer 2004-05, nr. 51-1465/002; *http://www.raadvst-consetat.be/dbx/adviezen/37904.pdf*).

Article 48

À l'article XI.125/7, 2°, en projet, les mots ", par exemple en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle" seront remplacés par les mots "en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou de toute autre manière"[10].

*

Le greffier, *Le président,*

Béatrice DRAPIER Pierre VANDERNOOT

Artikel 48

In het ontworpen artikel XI.125/7, 2°, moeten de woorden ", bijvoorbeeld door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken" worden vervangen door de woorden "door te weigeren de naar aanleiding van deze inspectie of anderszins gevraagde informatie te verstrekken"[10].

*

De griffier, *De voorzitter,*

Béatrice DRAPIER Pierre VANDERNOOT

[10] Voir l'observation formulée sous l'article 28 de l'avant-projet.

[10] Zie de opmerking over artikel 28 van het voorontwerp.

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, du ministre des Finances, chargé de la Coordination de la lutte contre la fraude et de la ministre des Télécommunications et de la Poste,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le premier ministre, le ministre de l'Économie, le ministre des Finances, chargé de la Coordination de la lutte contre la fraude et la ministre des Télécommunications et de la Poste sont chargés de présenter en Notre nom à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1ER

Définitions et dispositions générales

Section 1re

Objet et champ d'application

Sous-section 1re. – Objet

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

La présente loi met en œuvre partiellement le 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, ci-après: le "Règlement sur la cybersécurité".

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, de minister van Financiën, belast met de Coördinatie van de fraudebestrijding en de minister van Telecommunicatie en Post,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De eerste minister, de minister van Economie, de minister van Financiën, belast met de Coördinatie van de fraudebestrijding en de minister van Telecommunicatie en Post 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

Definities en algemene bepalingen

Afdeling 1

Onderwerp en toepassingsgebied

Onderafdeling 1. – Onderwerp

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

Deze wet geeft gedeeltelijk uitvoering aan 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, hierna: de "Cyberbeveiligingsverordening".

Sous-section 2. – Champ d'application

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.

§ 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 d'une telle certification, 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 d'une telle certification.

§ 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 au sens de 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 ("loi NIS"), de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la protection et la sécurité des infrastructures critiques et de l'article 2, 1°, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

Dans le respect des dispositions légales applicables et du paragraphe 2, les autorités précitées 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 par la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique ni à la FSMA visée par 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.

Onderafdeling 2. – Toepassingsgebied

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.

§ 2. De hoofdstukken 1 tot 4, 7 en 8, alsook de artikelen 21 en 22, zijn ook van toepassing op een Europese cyberbeveiligingscertificering die wordt opgelegd.

Bij de uitvoering van artikel 21 en 22 in het kader van een dergelijke certificering zijn artikel 19 en 26 van toepassing.

De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, hoofdstuk 5 en 6 volledig of gedeeltelijk toepasselijk maken in het kader van deze 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 als bedoeld 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 ("NIS-wet"), 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, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

Met inachtneming van de toepasselijke wettelijke bepalingen en van paragraaf 2 zorgen de voornoemde 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.

§ 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.

Section 2

Définitions

Art. 4

Pour l'application de la présente loi, il faut entendre par:

1° "autorité nationale de certification de cybersécurité": l'autorité visée à l'article 58 du Règlement sur la cybersécurité et désignée par le Roi conformément à l'article 5, § 1er;

2° "GECC": Groupe européen de certification de cybersécurité visé à l'article 62 du Règlement sur la cybersécurité;

3° "autorité nationale d'accréditation": l'organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique et visé à l'article 2, 16°, du Règlement sur la cybersécurité;

4° "autorité publique": l'autorité publique au sens de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

5° "service d'inspection": le service d'inspection visé à l'article 13, § 1er.

CHAPITRE 2

Autorités compétentes et coopération au niveau national

Section 1re

Autorités compétentes

Art. 5

§ 1er. Le Roi désigne l'autorité qui est chargée, en tant qu'autorité nationale de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et par la présente loi.

§ 2. En fonction de l'objet du schéma de certification concerné et à la demande de l'autorité publique concernée, le Roi peut, par dérogation, confier, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6 de l'autorité

Afdeling 2

Definities

Art. 4

Voor de toepassing van deze wet moet worden verstaan onder:

1° "nationale cyberbeveiligingscertificeringsautoriteit": de autoriteit bedoeld in artikel 58 van de Cyberbeveiligingsverordening die is aangewezen door de Koning overeenkomstig artikel 5, § 1;

2° "EGC": Europese Groep voor cyberbeveiligingscertificering bedoeld in artikel 62 van de Cyberbeveiligingsverordening;

3° "nationale accreditatieautoriteit": de instelling bedoeld in artikel 2, 16°, van de Cyberbeveiligingsverordening die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;

4° "overheid": de overheid als bedoeld in artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

5° "inspectiedienst": de inspectiedienst bedoeld in artikel 13, § 1.

HOOFDSTUK 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

Afdeling 1

Bevoegde autoriteiten

Art. 5

§ 1. De Koning wijst de autoriteit aan die, als nationale cyberbeveiligingscertificeringsautoriteit, belast is met de taken en opdrachten bedoeld in de Cyberbeveiligingsverordening en in deze wet.

§ 2. Naargelang het voorwerp van de betrokken certificeringsregeling en op verzoek van de betrokken overheid kan de Koning, bij wijze van afwijking en bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6 van de autoriteit

visée au paragraphe 1er à une autre autorité publique, à l'exception des articles 21 et 22.

Le Roi veille à tenir compte de l'expertise de l'autorité publique concernée lors de l'attribution éventuelle de tâches de contrôle.

§ 3. Dans l'hypothèse visée au paragraphe 2, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée au paragraphe 1er et l'autorité publique concernée.

§ 4. Dans l'exercice de ces missions confiées par le Roi et sans préjudice de ses compétences légales en matière de contrôle et de sanctions, l'autorité publique concernée dispose des mêmes droits et obligations que ceux visés aux chapitres 5 et 6.

Section 2

Coopération au niveau national

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.

§ 2. Conformément à l'article 58, § 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 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 sanction et de réclamation. Lorsqu'un échange d'informations porte

bedoeld in paragraaf 1, volledig of gedeeltelijk toevertrouwen aan een andere overheid, met uitzondering van artikel 21 en 22.

De Koning houdt rekening met de expertise van de betrokken overheid bij de eventuele toekenning van toezichtstaken.

§ 3. In het in paragraaf 2 bedoelde geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in paragraaf 1 en de betrokken overheid.

§ 4. Bij de uitoefening van deze door de Koning toevertrouwde opdrachten en onverminderd haar wettelijke toezichts- en sanctiebevoegdheden beschikt de betrokken overheid over dezelfde rechten en verplichtingen als die bedoeld in hoofdstuk 5 en 6.

Afdeling 2

Samenwerking op nationaal niveau

Art. 6

§ 1. De autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 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 hoofdstuk 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 autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen en, anderzijds, de sectorale overheden en de inspectiediensten, respectievelijk bedoeld in artikel 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 artikel 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

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 BSA-ANS 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 du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, aux 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, à l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien 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.

§ 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.

Il s'agit des informations nécessaires en matière de contrôle, de sanction et de réclamation. Lorsque ces informations portent sur des données à caractère

en klachten. Indien een informatie-uitwisseling persoonsgegevens betreft, gebeurt deze overeenkomstig de bepalingen van hoofdstuk 8. De modaliteiten 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 hoofdstuk 5 en 6 door de Koning is aangewezen verstrekken de ontvangers, namelijk een sectorale overheid, een inspectiedienst, de luchthaveninspectie, de luchtvaartinspectie of de BSA-ANS, 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 deze informatie betrekking heeft op een inbreuk op artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, 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, artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer of afdeling 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 paragraaf 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 hoofdstuk 5 en 6 door de Koning is aangewezen, indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.

Het gaat om noodzakelijke informatie met betrekking tot toezicht, sancties en klachten. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing.

personnel, le chapitre 8 est d'application. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

Art. 7

Dans le cadre des missions et pouvoirs qui leur sont attribués par la loi, les autorités publiques peuvent assister l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, dans ses missions de contrôle visées par la présente loi.

CHAPITRE 3

Autorité nationale de certification de cybersécurité

Section 1re

Représentation au Groupe européen de certification de cybersécurité

Art. 8

§ 1er. L'autorité visée à l'article 5, § 1er, représente la Belgique au sein du GECC.

§ 2. Dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité visée à l'article 5, § 1er, se concerte avec les autres autorités publiques désignées par le Roi, en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma de certification candidat au sens de l'article 49 du Règlement sur la cybersécurité.

§ 3. D'autres autorités publiques peuvent assister avec l'autorité visée à l'article 5, § 1er, aux travaux et réunions du GECC.

Section 2

Indépendance

Art. 9

§ 1er. L'autorité visée à l'article 5, § 1er, prend les mesures nécessaires afin d'assurer l'indépendance des membres de son personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de ses tâches de contrôle ou de certification en matière de cybersécurité, afin d'éviter

De modaliteiten van de informatie-uitwisseling waarborgen de vertrouwelijkheid van de betrokken informatie.

Art. 7

De overheden mogen, in het kader van de opdrachten en bevoegdheden die hun zijn toevertrouwd door de wet, de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, bijstaan bij de in deze wet bedoelde toezichtsopdrachten.

HOOFDSTUK 3

Nationale cyberbeveiligingscertificeringsautoriteit

Afdeling 1

Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering

Art. 8

§ 1. De autoriteit bedoeld in artikel 5, § 1, vertegenwoordigt België in de EGC.

§ 2. In het kader van haar opdracht om België in de EGC te vertegenwoordigen overlegt de autoriteit bedoeld in artikel 5, § 1, met de andere door de Koning aangewezen overheden, met name bij de voorbereiding en goedkeuring van een advies over een potentiële certificeringsregeling als bedoeld in artikel 49 van de Cyberbeveiligingsverordening.

§ 3. Andere overheden kunnen, samen met de autoriteit bedoeld in artikel 5, § 1, de werkzaamheden en vergaderingen van de EGC bijwonen.

Afdeling 2

Onafhankelijkheid

Art. 9

§ 1. De autoriteit bedoeld in artikel 5, § 1, neemt de nodige maatregelen om, bij de uitvoering van haar toezichts- of certificeringstaken op het gebied van cyberbeveiliging, de onafhankelijkheid van haar personeelsleden te garanderen, belangenconflicten doeltreffend te voorkomen, te identificeren en op te lossen, teneinde

des distorsions de concurrence et de garantir l'égalité de traitement de tous.

La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel de l'autorité visée à l'article 5, § 1er, chargé de la certification ou du contrôle a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.

§ 2. Les membres du personnel de l'autorité visée à l'article 5, § 1er, ne reçoivent ni ne cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne.

Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.

Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

CHAPITRE 4

Délivrance des certificats européens

Section 1re

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élémentaire" ou "substantiel"

Art. 10

§ 1er. Conformément à l'article 56, § 4, du Règlement sur la cybersécurité, les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élémentaire" ou "substantiel".

§ 2. Conformément à l'article 56, § 5, a), du Règlement sur la cybersécurité, lorsque le schéma européen de certification de cybersécurité l'impose, la délivrance de tels certificats est réservée à l'autorité visée à l'article 5, § 1er.

§ 3. Conformément à l'article 56, § 5, b), du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, peut néanmoins déléguer en tout ou en partie la délivrance d'un

vertekening van de mededinging te vermijden en de gelijke behandeling van allen te waarborgen.

Het begrip "belangenconflict" heeft minstens betrekking op situaties waarin een met de certificering of het toezicht belast personeelslid van de autoriteit bedoeld in artikel 5, § 1, rechtstreeks of onrechtstreeks financiële, economische of andere persoonlijke belangen heeft die geacht kunnen worden zijn onpartijdigheid en onafhankelijkheid in het kader van zijn opdracht of functie in het gedrang te brengen.

§ 2. De personeelsleden van de autoriteit bedoeld in artikel 5, § 1, krijgen noch vragen binnen de grenzen van hun bevoegdheden op directe of indirecte wijze van niemand instructies.

Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarin zij een persoonlijk of rechtstreeks belang hebben of waarin hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben.

De Koning kan ook andere situaties benoemen als belangenconflicten.

HOOFDSTUK 4

Afgifte van Europese certificaten

Afdeling 1

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"

Art. 10

§ 1. Overeenkomstig artikel 56, lid 4, van de Cyberbeveiligingsverordening geven de conformiteitsbeoordelingsinstanties die door de nationale accreditatieautoriteit geaccrediteerd zijn, de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel" af.

§ 2. Overeenkomstig artikel 56, lid 5, onder a), van de Cyberbeveiligingsverordening is de afgifte van deze certificaten, indien vereist door de Europese cyberbeveiligingscertificeringsregeling, voorbehouden aan de autoriteit bedoeld in artikel 5, § 1.

§ 3. Overeenkomstig artikel 56, lid 5, onder b), van de Cyberbeveiligingsverordening kan de autoriteit bedoeld in artikel 5, § 1, naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie, de afgifte van een certificaat bedoeld in paragraaf 2 niettemin

certificat visé au paragraphe 2 à un organisme public accrédité par l'autorité nationale d'accréditation en tant qu'organisme d'évaluation de la conformité.

Section 2

Certificats de cybersécurité européens attestant d'un niveau d'assurance "élevé"

Art. 11

§ 1er. Conformément à l'article 56, § 6, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit "élevé".

§ 2. Conformément à l'article 56, § 6, b), du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, peut toutefois déléguer en tout ou en partie cette tâche à un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation.

Section 3

Réclamation en cas de refus de délivrance

Art. 12

Conformément à l'article 63, § 1er, du Règlement sur la cybersécurité, en cas de refus de délivrance d'un certificat de cybersécurité européen par l'autorité visée à l'article 5, § 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation prévue à l'article 10, § 3, ou à l'article 11, § 2, le demandeur peut introduire une réclamation devant l'autorité visée à l'article 5, § 1er, selon les modalités prévues au chapitre 7.

CHAPITRE 5

Contrôle

Art. 13

§ 1er. Conformément à l'article 58, § 7 et § 8, 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 disposent chacun d'un service d'inspection qui peut à tout moment réaliser des contrôles du respect par les organismes d'évaluation de la conformité,

volledig of gedeeltelijk delegeren aan een overheidsinstelling die door de nationale accreditatieautoriteit als conformiteitsbeoordelingsinstantie geaccrediteerd is.

Afdeling 2

Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"

Art. 11

§ 1. Overeenkomstig artikel 56, lid 6, van de Cyberbeveiligingsverordening geeft de autoriteit bedoeld in artikel 5, § 1, de Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog" af.

§ 2. Overeenkomstig artikel 56, lid 6, onder b), van de Cyberbeveiligingsverordening kan de autoriteit bedoeld in artikel 5, § 1, naargelang de technische vereisten van de certificeringsregeling en na voorafgaande delegatie, deze taak echter volledig of gedeeltelijk delegeren aan een conformiteitsbeoordelingsinstantie die door de nationale accreditatieautoriteit geaccrediteerd is.

Afdeling 3

Klacht ingeval de afgifte geweigerd wordt

Art. 12

Overeenkomstig artikel 63, lid 1, van de Cyberbeveiligingsverordening kan de aanvrager, ingeval de afgifte van een Europees cyberbeveiligingscertificaat geweigerd wordt door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie bedoeld in artikel 10, § 3, of in artikel 11, § 2, een klacht indienen bij de autoriteit bedoeld in artikel 5, § 1, volgens de in hoofdstuk 7 bepaalde modaliteiten.

HOOFDSTUK 5

Toezicht

Art. 13

§ 1. Overeenkomstig artikel 58, lid 7 en lid 8, van de Cyberbeveiligingsverordening beschikken de autoriteit bedoeld in artikel 5, § 1, en de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, elk over een inspectiedienst die op elk ogenblik controles kan uitvoeren om na te gaan of de conformiteitsbeoordelingsinstanties, de houders van vrijwillige

les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le règlement sur la cybersécurité, les schémas européens de certification de cybersécurité, la présente loi ou ses arrêtés d'exécution.

Les compétences de ce service d'inspection sont sans préjudice de l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.

Conformément à l'article 58, § 4, du Règlement sur la cybersécurité, dans l'exécution de ses tâches de contrôle, le service d'inspection agit de manière indépendante des autres services de l'autorité visée à l'article 5, § 1er, notamment du service chargé de la délivrance des certificats de cybersécurité, ou des autres services de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 2. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande, les dispositions légales ainsi que, le cas échéant, la ou les parties du schéma européen de certification de cybersécurité et précise le délai dans lequel les informations ou preuves doivent être fournies.

§ 3. En fonction des caractéristiques propres à chaque schéma européen de certification de cybersécurité, le service d'inspection peut faire appel à des experts, lesquels sont soumis au secret professionnel prévu par le paragraphe 4.

Les frais de recours à des experts peuvent être mis à charge des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens ou des émetteurs de déclarations de conformité de l'Union européenne.

§ 4. Les membres du personnel du service d'inspection sont tenus au secret professionnel en ce qui concerne les informations en rapport à l'exécution de la présente loi.

Art. 14

Lorsqu'un organisme d'évaluation de la conformité, un titulaire de certificats de cybersécurité européens volontaires ou un émetteur de déclarations de conformité de l'Union européenne est situé en dehors du territoire belge, le service d'inspection peut solliciter la coopération et l'assistance des autorités nationales de certification de cybersécurité compétentes de ces autres États.

Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen de regels naleven die zijn opgelegd door de Cyberbeveiligingsverordening, de Europese cyberbeveiligingscertificeringsregelingen, deze wet of de uitvoeringsbesluiten ervan.

De bevoegdheden van deze inspectiedienst doen geen afbreuk aan de toepassing van het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling.

Overeenkomstig artikel 58, lid 4, van de Cyberbeveiligingsverordening handelt de inspectiedienst bij de uitvoering van zijn toezichtstaken onafhankelijk van de andere diensten van de autoriteit bedoeld in artikel 5, § 1, met name van de dienst belast met de afgifte van cyberbeveiligingscertificaten, of van de andere diensten van de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen.

§ 2. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doeleinde van het verzoek, de wettelijke bepalingen en, in voorkomend geval, het deel of de delen van de Europese cyberbeveiligingscertificeringsregeling, alsook de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

§ 3. Naargelang de specifieke kenmerken van elke Europese cyberbeveiligingscertificeringsregeling kan de inspectiedienst een beroep doen op experten die onderworpen zijn aan het in paragraaf 4 bedoelde beroepsgeheim.

De kosten om een beroep te doen op experten kunnen ten laste worden gelegd van de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen.

§ 4. De personeelsleden van de inspectiedienst zijn gebonden aan het beroepsgeheim wat de informatie in verband met de uitvoering van deze wet betreft.

Art. 14

Wanneer een conformiteitsbeoordelingsinstantie, een houder van vrijwillige Europese cyberbeveiligingscertificaten of een afgever van EU-conformiteitsverklaringen zich buiten het Belgische grondgebied bevindt, kan de inspectiedienst de bevoegde nationale cyberbeveiligingscertificeringsautoriteiten van deze andere landen om samenwerking en bijstand verzoeken.

Art. 15

§ 1er. Les membres assermentés du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi.

§ 2. Les membres assermentés du service d'inspection ou les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les organismes d'évaluation de la conformité, titulaires de certificats de cybersécurité européens ou émetteurs de déclarations de conformité de l'Union européenne qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

§ 3. Afin de mener à bien les activités de supervision visées à l'article 58 du Règlement sur la cybersécurité et 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 disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission:

1° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens ou l'émetteur de déclarations de conformité de l'Union européenne; ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction;

2° prendre connaissance sur place et obtenir une copie du certificat ou de la déclaration de conformité de l'Union européenne, ainsi que de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission;

3° procéder à tout examen, contrôle et audition, et requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission;

4° relever et vérifier l'identité des personnes qui se trouvent sur les lieux utilisés par l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens ou l'émetteur de déclarations de conformité de l'Union européenne 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;

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection adressent une demande motivée au juge

Art. 15

§ 1. De beëdigde leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model door de Koning wordt bepaald.

§ 2. De beëdigde leden van de inspectiedienst of de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de conformiteitsbeoordelingsinstanties, de houders van Europese cyberbeveiligingscertificaten of de afgevers van EU-conformiteitsverklaringen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Ze leggen de eed af bij de leidend ambtenaar van hun dienst.

§ 3. Om de toezichthoudende werkzaamheden bedoeld in artikel 58 van de Cyberbeveiligingsverordening uit te voeren en onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering, beschikken de beëdigde leden van de inspectiedienst op elk ogenblik over de volgende toezichtsbevoegdheden bij de uitoefening van hun opdracht:

1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de conformiteitsbeoordelingsinstantie, de houder van Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits vooraf een machtiging is uitgereikt door de onderzoeksrechter;

2° ter plaatse kennisnemen van het certificaat of de EU-conformiteitsverklaring, alsook van alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht en hiervan een kopie verkrijgen;

3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht;

4° de identiteit opnemen en controleren van de personen die zich bevinden op de plaatsen die de conformiteitsbeoordelingsinstantie, de houder van Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen gebruikt 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;

§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst een met redenen omkleed verzoek aan

d'instruction. Cette demande contient au moins les données suivantes:

1° l'identification des espaces habités auxquels les membres du personnel du service d'inspection souhaitent avoir accès;

2° les infractions présumées qui font l'objet du contrôle;

3° la législation qui donne lieu au contrôle pour lequel les inspecteurs estiment nécessaire d'obtenir une autorisation de visite;

4° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire;

5° la proportionnalité et la subsidiarité à l'égard de tout autre devoir d'enquête.

Le juge d'instruction décide dans un délai de 48 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. Le service d'inspection 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 assermentés du service d'inspection agissant conjointement.

§ 5. 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.

de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe de personeelsleden van de inspectiedienst toegang wensen te hebben;

2° de vermoedelijke inbreuken die het voorwerp zijn van de controle;

3° de wetgeving die aanleiding geeft tot de controle waarvoor de inspecteurs een machtiging tot bezoek menen nodig hebben;

4° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is;

5° de proportionaliteit en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

De onderzoeksrechter beslist binnen een termijn van maximum 48 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. De 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 beëdigde leden van de inspectiedienst die samen optreden.

§ 5. 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 geeft, 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.

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 à 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 personnel du service d'inspection qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 6. Les membres du service d'inspection peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée.

S'il n'est pas possible de prendre des copies sur place, les membres du service d'inspection peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 7. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 6, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection peut solliciter l'autorisation d'un juge d'instruction, selon les mêmes conditions que celles prévues au paragraphe 4.

§ 8. Lorsque cela s'avère nécessaire, les membres du service d'inspection disposent d'une habilitation de sécurité correspondant au niveau de classification, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, des informations auxquelles ils doivent avoir accès afin de réaliser leur contrôle.

§ 9. Lorsque cela est nécessaire à la réalisation des activités de contrôle visées au présent chapitre et que les autres moyens ne suffisent pas, les membres assermentés du service d'inspection peuvent avoir accès aux informations ou secrets visés à l'article 458 du Code pénal et dont un titulaire de certificats de cybersécurité européens ou un émetteur de déclarations de conformité de l'Union européenne est le dépositaire, et les traiter.

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 personeelsleden van de inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 6. De leden van de inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 7. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst de toestemming vragen van een onderzoeksrechter, volgens dezelfde voorwaarden als die bedoeld in paragraaf 4.

§ 8. Indien nodig beschikken de leden van de inspectiedienst over een veiligheidsmachtiging die overeenstemt met het classificatieniveau, als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de informatie waar zij toegang toe moeten hebben om hun controle uit te voeren.

§ 9. Indien dit nodig is voor de uitvoering van de toezichtsactiviteiten bedoeld in dit hoofdstuk en de andere middelen niet volstaan, kunnen de beëdigde leden van de inspectiedienst toegang krijgen tot de informatie of geheimen bedoeld in artikel 458 van het Strafwetboek en deze verwerken, wanneer een houder van Europese cyberbeveiligingscertificaten of een afgever van EU-conformiteitsverklaringen er kennis van draagt.

§ 10. Lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les membres assermentés du service d'inspection veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour le contrôle des dispositions du Règlement sur la cybersécurité ou d'un schéma de certification dont ils contrôlent le respect.

Art. 16

§ 1er. À 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.

§ 3. À 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, § 7, c), et 60, § 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 prévu 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 précédent ne doit pas être formalisée par un protocole pour autant que:

1° le transfert soit nécessaire à l'exécution de l'alinéa précédent;

2° l'autorité destinataire des données traite celles-ci afin d'assurer le respect des dispositions de la loi, des articles 58, § 7, c), et 60, § 1er et § 4, du Règlement sur la cybersécurité ou des articles 107/2 à 107/5 de

§ 10. Bij de uitvoering van hun toezichtsbevoegdheden bedoeld in dit artikel zorgen de beëdigde leden van de inspectiedienst ervoor dat de door hen gebruikte middelen passend en noodzakelijk zijn voor het toezicht op de bepalingen van de Cyberbeveiligingsverordening of een certificeringsregeling waarvan zij de naleving controleren.

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.

§ 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, lid 1 en lid 4, van de Cyberbeveiligingsverordening of in artikel 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 vorige lid niet worden geformaliseerd aan de hand van een protocol voor zover:

1° de doorgifte noodzakelijk is voor de uitvoering van het vorige 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, lid 1 en lid 4, van de Cyberbeveiligingsverordening of van 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;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format digital ou papier.

§ 4. Afin d'assurer 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 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 d'information d'intérêt général pour la sécurité publique, 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 du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou 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'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 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 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 BSA-ANS, au sens des articles 2, alinéa 1er, 1° et 9°, et 15, § 1er à § 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures

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, voornaam, particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

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 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 wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en 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, 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 wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of 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.

Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en afdeling 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 BSA-ANS, als bedoeld in de artikelen 2, eerste lid, 1° en 9°, en 15, § 1 tot § 3, van het koninklijk

critiques dans le sous-secteur du transport aérien, lorsque ce rapport est lié à un contrôle effectué auprès d'une infrastructure critique, au sens de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.

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 précédent;

2° l'autorité destinataire des données traite celles-ci afin d'assurer 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;

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 digital ou papier.

Art. 17

§ 1er. Les membres assermentés du service d'inspection rédigent des procès-verbaux visés à l'article 20, § 1er.

§ 2. À 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, § 7, c), et 60, § 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

besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, indien dit verslag betrekking heeft op een controle bij een kritieke infrastructuur als bedoeld in het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer.

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:

1° de doorgifte noodzakelijk is voor de uitvoering van het vorige 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;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, voornaam, particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

Art. 17

§ 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, lid 1 en lid 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

belge des services postaux et des télécommunications peut recevoir 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 précédent ne doit pas être formalisée par un protocole pour autant que:

1° le transfert soit nécessaire à l'exécution de l'alinéa précédent;

2° l'autorité destinataire des données traite celles-ci afin d'assurer le respect des dispositions de la loi, des articles 58, § 7, c), et 60, § 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;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format digital ou papier.

§ 3. Afin d'assurer 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 du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et 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, 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

accreditatieautoriteit of het Belgisch Instituut voor postdiensten en telecommunicatie een kopie krijgen 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.

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 vorige lid niet worden geformaliseerd aan de hand van een protocol voor zover:

1° de doorgifte noodzakelijk is voor de uitvoering van het vorige 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, lid 1 en lid 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, voornaam, particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

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 wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en 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, 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 infrastructuur, aanbieder van essentiële

numérique au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou 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'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 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 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 du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, à l'inspection aéroportuaire, à l'inspection aéronautique ou à la BSA-ANS, au sens des 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.

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 précédent;

2° l'autorité destinataire des données traite celles-ci afin d'assurer 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;

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;

diensten of digitaledienstverlener als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of 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.

Met inachtneming van artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer en afdeling 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 koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, aan de luchthaveninspectie, de luchtvaartinspectie of de BSA-ANS, als bedoeld 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.

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 vorige 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;

3° de doorgifte betrekking heeft op persoonlijke identificatiegegevens zoals een naam, voornaam, particulier of professioneel e-mailadres, authenticatiegegevens of elektronische-communicatiegegevens;

4° le transfert de données à caractère personnel se fasse de manière sécurisée dans un format digital ou papier.

Art. 18

§ 1er. Conformément aux articles 53, § 3, et 58, § 8, a), du Règlement sur la cybersécurité, l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens volontaires ou l'émetteur de déclarations de conformité de l'Union européenne apporte son entière collaboration aux membres du service d'inspection ou aux experts appelés à participer à l'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes.

Si nécessaire, l'organisme d'évaluation de la conformité, le titulaire de certificats de cybersécurité européens volontaires ou l'émetteur de déclarations de conformité de l'Union européenne met à disposition des membres du service d'inspection et des experts appelés à participer à l'inspection le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Après avis de l'autorité visée à l'article 5, § 1er, le Roi peut déterminer des rétributions relatives à la délivrance et aux prestations d'inspections réalisées dans le cadre du recours volontaire à des certifications et déclarations de conformité visées par le Règlement sur la cybersécurité.

Ces rétributions sont à charge des organismes d'évaluation de la conformité, titulaires de certificats de cybersécurité européens volontaires et des émetteurs de déclarations de conformité de l'Union européenne. Le Roi fixe les modalités de calcul et de paiement.

CHAPITRE 6

Sanctions

Section 1re

Procédure

Art. 19

§ 1er. Lorsqu'un ou plusieurs manquements aux exigences imposées par le Règlement sur la cybersécurité, la présente loi ou ses arrêtés d'exécution ou aux exigences de schémas de certification volontaire de cybersécurité sont constatés, le service d'inspection met en demeure le

4° de doorgifte van persoonsgegevens beveiligd verloopt in een digitaal of papieren formaat.

Art. 18

§ 1. Overeenkomstig de artikelen 53, lid 3, en 58, lid 8, onder a), van de Cyberbeveiligingsverordening verleent de conformiteitsbeoordelingsinstantie, de houder van vrijwillige Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen volledige medewerking aan de leden van de inspectiedienst of de experten die deelnemen aan de inspectie bij de uitoefening van hun functie, met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de conformiteitsbeoordelingsinstantie, de houder van vrijwillige Europese cyberbeveiligingscertificaten of de afgever van EU-conformiteitsverklaringen het nodige materiaal ter beschikking van de leden van de inspectiedienst en de experten die deelnemen aan de inspectie, zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. Na advies van de autoriteit bedoeld in artikel 5, § 1, kan de Koning retributies bepalen voor de afgifte en de inspectieprestaties die geleverd worden in het kader van het vrijwillige gebruik van certificeringen en conformiteitsverklaringen bedoeld in de Cyberbeveiligingsverordening.

Deze retributies zijn ten laste van de conformiteitsbeoordelingsinstanties, de houders van vrijwillige Europese cyberbeveiligingscertificaten en de afgevers van EU-conformiteitsverklaringen. De Koning bepaalt de nadere regels inzake berekening en betaling.

HOOFDSTUK 6

Sancties

Afdeling 1

Procedure

Art. 19

§ 1. Wanneer een of meer inbreuken op de voorschriften van de Cyberbeveiligingsverordening, deze wet of de uitvoeringsbesluiten ervan of op de voorschriften van vrijwillige cyberbeveiligingscertificeringsregelingen worden vastgesteld, maant de inspectiedienst de overtreder

contrevenant de se conformer, dans un délai raisonnable qu'il fixe, aux obligations qui lui incombent.

Le délai est déterminé en tenant compte des conditions de fonctionnement du contrevenant et des mesures à mettre en œuvre.

§ 2. Au préalable, le service d'inspection informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant son envoi par le service d'inspection.

Art. 20

§ 1er. Lorsque le service d'inspection constate que le contrevenant n'a pas respecté les obligations découlant de la loi ou du Règlement sur la cybersécurité, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection.

§ 2. Le fait pour quiconque d'empêcher ou entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté par les membres assermentés du service d'inspection dans un procès-verbal.

§ 3. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Section 2

Retrait d'un certificat

Art. 21

Conformément à l'article 58, § 8, e), du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, retire un certificat de cybersécurité lorsque le bénéficiaire ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

aan om zijn verplichtingen na te komen binnen een door hem vastgestelde redelijke termijn.

De termijn wordt bepaald rekening houdend met de werkingsomstandigheden van de overtreder en de te nemen maatregelen.

§ 2. De inspectiedienst deelt de overtreder vooraf, 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 vijftien 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 de zesde dag na de verzending ervan door de inspectiedienst.

Art. 20

§ 1. Als de inspectiedienst vaststelt dat de overtreder de verplichtingen van de wet of de Cyberbeveiligingsverordening niet is nagekomen, worden de feiten opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 2. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst opzettelijk verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of bewust foutieve of onvolledige informatie verstrekt, wordt opgetekend in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 3. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Afdeling 2

Intrekking van een certificaat

Art. 21

Overeenkomstig artikel 58, lid 8, e), van de Cyberbeveiligingsverordening trekt de autoriteit bedoeld in artikel 5, § 1, een cyberbeveiligingscertificaat in als de begunstigde de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Section 3

Limitation, suspension ou retrait d'une autorisation ou d'une délégation

Art. 22

Conformément à l'article 58, § 7, e), du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, limite, suspend ou retire les autorisations ainsi que les délégations qu'elle a accordées aux organismes d'évaluation de la conformité, lorsque le bénéficiaire de l'autorisation ou de la délégation ne respecte pas le Règlement sur la cybersécurité ou un schéma européen de certification de cybersécurité.

Section 4

Amendes administratives

Art. 23

§ 1er. Est puni d'une amende de 500 à 75 000 euros quiconque ne répond pas à une demande d'information de l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 2. Est puni d'une amende de 500 à 100 000 euros le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC qui ne se conforme pas aux dispositions relatives à l'autoévaluation de la conformité visées à l'article 53 du Règlement sur la cybersécurité.

§ 3. Est également puni d'une amende de 500 à 100 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 4. Est puni d'une amende de 500 à 125 000 euros le titulaire d'un certificat de cybersécurité européen attestant du niveau d'assurance dit "substantiel" ou "élevé" qui ne se conforme pas aux obligations émanant du schéma européen de certification de cybersécurité correspondant.

§ 5. Sans préjudice de l'article 15, § 5, alinéa 1er, 3°, est puni d'une amende de 500 à 150 000 euros quiconque ne coopère pas lors d'un contrôle en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou ne coopère pas lors d'un contrôle de toute autre manière.

Afdeling 3

Beperken, opschorten of intrekken van een toelating of een delegatie

Art. 22

Overeenkomstig artikel 58, lid 7, e), van de Cyberbeveiligingsverordening voorziet de autoriteit bedoeld in artikel 5, § 1, in de beperking, opschorting of intrekking van toelatingen alsook van delegaties die ze aan conformiteitsbeoordelingsinstanties heeft verleend, als de begunstigde van de toelating of delegatie de Cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling niet naleeft.

Afdeling 4

Administratieve geldboetes

Art. 23

§ 1. Eenieder die niet reageert op een verzoek om informatie van de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, wordt gestraft met een geldboete van 500 tot 75 000 euro.

§ 2. De fabrikant of aanbieder van ICT-producten, -diensten of -processen die niet voldoet aan de bepalingen inzake conformiteitszelfbeoordeling bedoeld in artikel 53 van de Cyberbeveiligingsverordening, wordt gestraft met een geldboete van 500 tot 100 000 euro.

§ 3. De houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling, wordt eveneens gestraft met een geldboete van 500 tot 100 000 euro.

§ 4. De houder van een Europees cyberbeveiligingscertificaat voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling, wordt gestraft met een geldboete van 500 tot 125 000 euro.

§ 5. Onverminderd artikel 15, § 5, eerste lid, 3°, wordt eenieder die niet meewerkt tijdens een inspectie door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken, of die anderszins weigert mee te werken tijdens een inspectie, gestraft met een geldboete van 500 tot 150 000 euro.

§ 6. Est puni d'une amende de 500 à 200 000 euros quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi et de ses arrêtés d'exécution.

Art. 24

§ 1er. La décision d'imposer une amende administrative mentionne le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, informe au préalable le contrevenant de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les quinze jours de la réception de la proposition, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. La proposition est présumée reçue par le contrevenant le sixième jour suivant son envoi par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

§ 3. En tenant compte des moyens de défense invoqués dans le délai visé au paragraphe 2 ou en l'absence de réaction du contrevenant dans ce même délai, l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, peut adopter une sanction administrative visée à l'article 23.

§ 4. L'amende administrative est proportionnelle à la gravité, la durée, les moyens utilisés, les dommages causés et les circonstances des faits.

L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

§ 5. Le concours de plusieurs infractions peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 25

La décision est notifiée par envoi recommandé au contrevenant.

Une invitation à acquitter l'amende dans un délai d'un mois est jointe à la décision.

§ 6. Eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening, deze wet en de uitvoeringsbesluiten ervan, wordt gestraft met een boete van 500 tot 200 000 euro.

Art. 24

§ 1. De beslissing om een administratieve geldboete op te leggen vermeldt het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen vijftien 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 de zesde dag na de verzending ervan door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen.

§ 3. Rekening houdend met de verweermiddelen die zijn aangevoerd binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, een in artikel 23 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 van dezelfde feiten 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. 25

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. 26

Le contrevenant peut contester la décision prise en vertu du chapitre 6 par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1er, ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Art. 27

§ 1er. Lorsque le contrevenant reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité visée l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, peut décerner une contrainte.

La contrainte est décernée par le représentant légal de l'autorité visée à l'article 5, § 1er, ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les vingt-quatre heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies.

L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation 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,

Art. 26

De overtreder kan de beslissing die de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, krachtens hoofdstuk 6 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

Het Marktenhof spreekt zich uit over de grond van de zaak en beschikt over volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Art. 27

§ 1. Als de overtreder de administratieve geldboete niet betaalt binnen de toegestane termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaardersexploot 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 van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld

par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte.

Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et l'article 55 de ce Code.

L'exercice de l'opposition à la contrainte suspend l'exécution de la contrainte, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire.

Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant.

Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 28

L'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, ne peut imposer d'amende administrative à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis.

in hoofdstuk 5 en 6 door de Koning is aangewezen, bij deurwaardersexploot 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.

§ 4. De autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, 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.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 28

De autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

CHAPITRE 7

Réclamations

Section 1re

Saisine de l'autorité nationale de certification de cybersécurité

Art. 29

Conformément à l'article 63, § 1er, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, reçoit et traite les réclamations liées à un certificat de cybersécurité européen délivré par l'autorité visée à l'article 5, § 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation prévue à l'article 10, § 3, ou 11, § 2, au refus de délivrance d'un tel certificat ou à une déclaration de conformité de l'Union européenne.

Art. 30

Le dépôt d'une réclamation par toute personne physique ou morale au sens de l'article 63 du Règlement sur la cybersécurité est sans frais.

Art. 31

§ 1er. L'autorité compétente examine si la réclamation est recevable.

§ 2. Une réclamation est recevable lorsqu'elle:

— est rédigée dans l'une des langues nationales;

— contient un exposé des faits et les indications nécessaires pour identifier le certificat de cybersécurité européen, le refus de délivrance d'un certificat ou la déclaration de conformité de l'Union européenne sur laquelle elle porte;

— relève de la compétence de l'autorité visée à l'article 5, § 1er, en vertu du Règlement sur la cybersécurité.

§ 3. L'autorité compétente peut inviter l'auteur de la réclamation à préciser sa réclamation.

Art. 32

L'affaire est traitée dans la langue nationale de la réclamation.

HOOFDSTUK 7

Klachten

Afdeling 1

Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit

Art. 29

Overeenkomstig artikel 63, lid 1, van de Cyberbeveiligingsverordening ontvangt en behandelt de autoriteit bedoeld in artikel 5, § 1, klachten van personen over een Europees cyberbeveiligingscertificaat dat is afgegeven door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie in het kader van de delegatie bedoeld in artikel 10, § 3, of 11, § 2, over de weigering om een dergelijk certificaat af te geven of over een EU-conformiteitsverklaring.

Art. 30

De indiening van een klacht door iedere natuurlijke of rechtspersoon als bedoeld in artikel 63 van de Cyberbeveiligingsverordening is kosteloos.

Art. 31

§ 1. De bevoegde autoriteit gaat na of de klacht ontvankelijk is.

§ 2. Een klacht is ontvankelijk wanneer zij:

— opgesteld is in een van de landstalen;

— een uiteenzetting van de feiten bevat, alsook de nodige indicaties voor de identificatie van het Europees cyberbeveiligingscertificaat, de weigering om een certificaat af te geven of de EU-conformiteitsverklaring waarop zij betrekking heeft;

— behoort tot de bevoegdheid van de autoriteit bedoeld in artikel 5, § 1, krachtens de Cyberbeveiligingsverordening.

§ 3. De bevoegde autoriteit kan de indiener van de klacht verzoeken zijn klacht toe te lichten.

Art. 32

De zaak wordt behandeld in de landstaal van de klacht.

Art. 33

La décision portant sur la recevabilité de la réclamation est portée à la connaissance de l'auteur de la réclamation.

Si l'autorité visée à l'article 5, § 1er, conclut à l'irrecevabilité de la réclamation, l'auteur de la réclamation en est informé.

Art. 34

Si l'autorité visée à l'article 5, § 1er, conclut à la recevabilité de la réclamation, elle peut exercer les pouvoirs qui lui sont conférés conformément aux articles 10, 11, 21 et 22.

L'autorité visée à l'article 5, § 1er, peut délivrer elle-même la certification demandée.

Section 2

Recours

Art. 35

Conformément à l'article 64, § 1er, du Règlement sur la cybersécurité, le réclamant peut contester la décision prise en vertu de la section 1re par l'autorité visée à l'article 5, § 1er, devant la Cour des marchés visée à l'article 101 du Code judiciaire.

La Cour des marchés est saisie du fond du litige et dispose d'une compétence de pleine juridiction.

La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité visée à l'article 5, § 1er.

La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.

Ce recours ne suspend pas l'exécution de la décision.

Art. 33

De beslissing inzake de ontvankelijkheid van de klacht wordt ter kennis gebracht van de indiener van de klacht.

Indien de autoriteit bedoeld in artikel 5, § 1, de klacht onontvankelijk verklaart, wordt de indiener van de klacht hierover ingelicht.

Art. 34

Indien de autoriteit bedoeld in artikel 5, § 1, de klacht ontvankelijk verklaart, kan zij de bevoegdheden uitoefenen die haar overeenkomstig de artikelen 10, 11, 21 en 22 zijn verleend.

De autoriteit bedoeld in artikel 5, § 1, kan zelf de gevraagde certificering afgeven.

Afdeling 2

Beroepen

Art. 35

Overeenkomstig artikel 64, lid 1, van de Cyberbeveiligingsverordening kan de indiener van de klacht de beslissing die de autoriteit bedoeld in artikel 5, § 1, krachtens afdeling 1 heeft genomen, betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

Het Marktenhof spreekt zich uit over de grond van de zaak en beschikt over volle rechtsmacht.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de autoriteit bedoeld in artikel 5, § 1, wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

CHAPITRE 8

Traitement des données à caractère personnel

Section 1re

Principes relatifs au traitement, base légale et finalités

Art. 36

§ 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;

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;

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 du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, 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;

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,

HOOFDSTUK 8

Verwerking van persoonsgegevens

Afdeling 1

Beginselen inzake verwerking, wettelijke basis en doeleinden

Art. 36

§ 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;

2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties overeenkomstig hoofdstuk 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;

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-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 wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren of in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, 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;

5° de samenwerking met de overheden die belast zijn met specifieke opdrachten inzake cyberbeveiliging, als bedoeld in artikel 2, 1), van de Cyberbeveiligingsverordening,

conformément à l'article 58, § 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.

§ 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, prénom, adresse, 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 chapitre 5 et 6.

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 indispensables aux missions de contrôle visées au chapitre 5.

Chaque fois que possible, les données visées à l'alinéa précédent sont pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le Règlement (UE) n° 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.

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, prénom, adresse, numéro de téléphone et adresse e-mail.

4° pour la finalité visée au paragraphe 1er, 4°, les données d'identification, c'est-à-dire le nom, prénom, adresse, numéro de téléphone et adresse e-mail ou de

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 hoofdstuk 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:

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 naam, voornaam, adres, telefoonnummer en 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 hoofdstuk 5 en 6.

De persoonsgegevens van klanten van houders van Europese cyberbeveiligingscertificaten of afgevers van EU-conformiteitsverklaringen, en de persoonsgegevens die deze klanten verwerken, mogen slechts worden verwerkt indien ze noodzakelijk zijn voor de toezichtsopdrachten bedoeld in hoofdstuk 5.

Indien mogelijk worden de gegevens bedoeld in het vorige lid gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met Verordening (EU) nr. 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.

3° voor het doeleinde bedoeld in paragraaf 1, 3°: de identificatiegegevens van natuurlijke personen die wensen deel te nemen aan de EGC, namelijk naam, voornaam, adres, telefoonnummer en e-mailadres.

4° voor het doeleinde bedoeld in paragraaf 1, 4°: de identificatiegegevens, namelijk naam, voornaam, adres, telefoonnummer en e-mailadres of

communications électroniques au sens de l'article 2, 89°, 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, prénom, adresse, numéro de téléphone et adresse e-mail ou de communications électroniques au sens de l'article 2, 89°, 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. Sans préjudice du paragraphe 3, 2°, les échanges d'informations entre autorités publiques prévus 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:

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;

elektronische-communicatiegegevens als bedoeld in artikel 2, 89°, 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 hoofdstuk 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 naam, voornaam, adres, telefoonnummer en e-mailadres of elektronische-communicatiegegevens als bedoeld in artikel 2, 89°, 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 hoofdstuk 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.

§ 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:

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;

3° toute personne physique introduisant une réclamation;

4° toute personne physique participant au GECC;

5° toute personne physique dont les données à caractère personnel sont présentes au sein des produits, services ou processus TIC, au sens de l'article 2, 12 à 14°, du Règlement sur la cybersécurité.

Art. 37

§ 1er. En application de l'article 23, § 1er, c), e) et h), du Règlement (UE) n° 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), certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent article. Ces limitations ou exclusions ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 16, 18 et 19 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel, effectués par l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, agissant en tant que responsable de traitement des données, pour la finalité visée à l'article 36, § 1er, 2°, dans la mesure où l'exercice des droits consacrés par ces articles nuirait aux besoins du contrôle ou des actes préparatoires à celui-ci.

§ 3. L'exemption vaut, sous réserve du principe de proportionnalité et le cas échéant de minimisation des données, pour toutes les catégories de données à caractère personnel, dans la mesure où le traitement de ces données n'est pas étranger aux finalités précitées. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 4. L'exemption ne s'applique que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'actes préparatoires à celui-ci, dans la mesure où l'exercice des droits faisant l'objet de la dérogation prévue au présent article nuirait aux besoins du contrôle ou des actes préparatoires à celui-ci et, en

3° iedere natuurlijke persoon die een klacht indient;

4° iedere natuurlijke persoon die deelneemt aan de EGC;

5° iedere natuurlijke persoon wiens persoonsgegevens gebruikt worden in ICT-producten, -diensten of -processen als bedoeld in artikel 2, 12° tot 14°, van de Cyberbeveiligingsverordening.

Art. 37

§ 1. Met toepassing van artikel 23, lid 1, onder c), e) en h), van Verordening (EU) nr. 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) worden bepaalde verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit artikel. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 16, 18 en 19 van voornoemde verordening zijn niet van toepassing op de verwerking van persoonsgegevens door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, die optreedt als verwerkingsverantwoordelijke voor het doeleinde bedoeld in artikel 36, § 1, 2°, voor zover de uitoefening van de in deze artikelen vastgelegde rechten nadelig zou zijn voor de controle of de voorbereidende werkzaamheden ervan.

§ 3. De uitzondering geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens, voor zover de verwerking van deze gegevens in overeenstemming is met voornoemde doeleinden. Deze uitzondering geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 4. De uitzondering geldt slechts voor de periode tijdens dewelke de betrokkene onderworpen is aan een controle of de voorbereidende werkzaamheden ervan, voor zover de uitoefening van de rechten die het voorwerp uitmaken van de in dit artikel bedoelde afwijking nadelig zou zijn voor de controle of de voorbereidende

tous les cas, ne s'applique que jusqu'à un an après réception de la demande d'exercice du droit faisant l'objet de la dérogation prévue au présent article.

La durée des actes préparatoires, visés à l'alinéa précédent, pendant laquelle les articles visés au paragraphe 2 ne sont pas applicables, ne peut excéder un an à partir de la réception d'une demande relative à l'application d'un des droits consacrés par ces articles.

§ 5. Dès réception d'une demande concernant l'exercice d'un des droits consacrés par les articles visés au paragraphe 2, le délégué à la protection des données du responsable du traitement en accuse réception.

Le délégué à la protection des données du responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation aux droits consacrés par les articles visés au paragraphe 2, ainsi que des motifs du refus ou de la limitation. Ces informations concernant le refus ou la limitation peuvent ne pas être fournies lorsque leur communication risque de compromettre la finalité énoncée au paragraphe 2. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

Le délégué à la protection des données du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'Autorité de protection des données et de former un recours juridictionnel.

Le délégué à la protection des données du responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'Autorité de protection des données.

Lorsque le service d'inspection a fait usage de l'exemption telle que déterminée au paragraphe 2, cette dernière est immédiatement levée après la clôture du contrôle. Le délégué à la protection des données du responsable du traitement en informe la personne concernée sans délai.

werkzaamheden ervan. In ieder geval geldt ze maximaal één jaar na ontvangst van het verzoek tot uitoefening van het recht dat het voorwerp uitmaakt van de in dit artikel bedoelde afwijking.

De duur van de voorbereidende werkzaamheden bedoeld in het vorige lid, tijdens dewelke de in paragraaf 2 bedoelde artikelen niet van toepassing zijn, is beperkt tot maximaal één jaar vanaf de ontvangst van een verzoek over de toepassing van een van de in deze artikelen vastgelegde rechten.

§ 5. Zodra de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke een verzoek ontvangt in verband met de uitoefening van een van de rechten die zijn vastgelegd in de artikelen bedoeld in paragraaf 2, bevestigt hij de ontvangst ervan.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene schriftelijk en onverwijld, in ieder geval binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van de rechten die zijn vastgelegd in de artikelen bedoeld in paragraaf 2, alsook over de redenen voor deze weigering of beperking. De informatie over de weigering of beperking kan achterwege worden gelaten wanneer de verstrekking ervan het doeleinde vermeld in paragraaf 2 zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal ervan kan die termijn indien nodig met twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van deze verlenging en van de redenen voor het uitstel.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de Gegevensbeschermingsautoriteit en om beroep in rechte in te stellen.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke vermeldt de feitelijke of juridische redenen waarop zijn beslissing steunt. Deze inlichtingen worden ter beschikking gesteld van de Gegevensbeschermingsautoriteit.

Wanneer de inspectiedienst een beroep heeft gedaan op de uitzondering bepaald in paragraaf 2, wordt deze onmiddellijk opgeheven na het afsluiten van de controle. De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke stelt de betrokkene daarvan onverwijld in kennis.

Section 2

Durée de conservation

Art. 38

Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, visé à l'article 89 du Règlement UE 2016/679, les données à caractère personnel traitées par l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 en vue de réaliser les finalités visées à l'article 36, § 1er, sont conservées, sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué.

CHAPITRE 9

Dispositions modificatives

Section 1re.

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 39

L'article 14, § 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, est complété par un 7° rédigé comme suit:

"7° L'Institut exerce les 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 [date] [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]."

Art. 40

Dans l'article 14, § 2, 3°, g), de la même loi, inséré par la loi du 10 juillet 2012 portant des dispositions diverses en matière de communications électroniques (cité comme: loi Télécom), les mots "en ce compris la sécurité des réseaux et des systèmes d'information," sont insérés entre les mots "sécurité publique," et "ou de sécurité et protection civile".

Afdeling 2

Bewaartermijn

Art. 38

Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening EU 2016/679, bewaart de verwerkingsverantwoordelijke de persoonsgegevens die verwerkt worden door de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen om de doeleinden bedoeld in artikel 36, § 1, te realiseren, onverminderd eventuele beroepsprocedures, gedurende 10 jaar na afloop van de verwerking.

HOOFDSTUK 9

Wijzigingsbepalingen

Afdeling 1.

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 39

Artikel 14, § 1, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector wordt aangevuld met een punt 7°, luidende:

"7° Het Instituut oefent 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 [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit]."

Art. 40

In artikel 14, § 2, 3°, g), van dezelfde wet, ingevoegd bij de wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische communicatie (aangehaald als: wet Telecom), worden de woorden "met inbegrip van de beveiliging van netwerk- en informatiesystemen," ingevoegd tussen de woorden "openbare veiligheid," en "of civiele veiligheid en bescherming".

Section 2

Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Art. 41

L'article 45 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers est complété par un paragraphe 6, rédigé comme suit:

"§ 6. À la demande de la FSMA et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la FSMA, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée et la FSMA. La FSMA exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu du paragraphe 1er, 2°, du présent article et des lois particulières qui régissent le contrôle des établissements financiers."

Art. 42

L'article 75, § 1er, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, est complété par un 27°, rédigé comme suit:

"27° à l'autorité visée à l'article 5, § 1er, de la loi du […] 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."

Section 3

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 43

Dans l'article 36/14, § 1er, de la loi du 22 février 1998 fixant le statut organique de la Banque

Afdeling 2

Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 41

Artikel 45 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een paragraaf 6, luidende:

"§ 6. Op verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit] volledig of gedeeltelijk aan de FSMA toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. De FSMA vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens paragraaf 1, 2°, van dit artikel en de bijzondere wetten die het toezicht op de financiële instellingen regelen."

Art. 42

Artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten wordt aangevuld met een punt 27°, luidende:

"27° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van […] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet."

Afdeling 3

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 43

In artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank

Nationale de Belgique, modifié en dernier lieu par la loi du 11 juillet 2021, il est inséré un 20°/2 rédigé comme suit:

"20°/2 dans les limites du droit de l'Union européenne, à l'autorité visée à l'article 5, § 1er, de la loi du […] 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;"

Art. 44

Dans le Chapitre IV/4 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, inséré par la loi du 7 avril 2019 et modifié en dernier lieu par la loi du 11 juillet 2021, il est inséré un article 36/48/1 rédigé comme suit:

"Art. 36/48/1. À la demande de la Banque et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la Banque, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée et la Banque. La Banque exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12*bis* et des lois particulières qui régissent le contrôle des établissements financiers."

Section 4

Modifications du Code de droit économique

Art. 45

L'article I.20 du Code de droit économique, inséré par la loi du 17 juillet 2013 et modifié par les lois du 1er décembre 2016 et du 15 avril 2018, est complété par un 10° rédigé comme suit:

"10° Règlement sur la cybersécurité: 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

van België, het laatst gewijzigd bij de wet van 11 juli 2021, wordt een punt 20°/2 ingevoegd, luidende:

"20°/2 binnen de grenzen van het recht van de Europese Unie, aan de autoriteit bedoeld in artikel 5, § 1, van de wet van […] 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;"

Art. 44

In Hoofdstuk IV/4 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij de wet van 7 april 2019 en het laatst gewijzigd bij de wet van 11 juli 2021, wordt een artikel 36/48/1 ingevoegd, luidende:

"Art. 36/48/1. Op verzoek van de Bank en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de Bank toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de Bank. De Bank vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12*bis* en de bijzondere wetten die het toezicht op de financiële instellingen regelen."

Afdeling 4

Wijzigingen van het Wetboek van economisch recht

Art. 45

Artikel I.20 van het Wetboek van economisch recht, ingevoegd bij de wet van 17 juli 2013 en gewijzigd bij de wetten van 1 december 2016 en 15 april 2018, wordt aangevuld met een punt 10°, luidende:

"10 °Cyberbeveiligingsverordening: 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 cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013."

Art. 46

Dans le livre XV, titre Ier, chapitre 2, du même Code, inséré par la loi du 18 avril 2017, il est inséré une section 10 intitulée "Section 10. Certification de cybersécurité".

Art. 47

Dans la section 10, insérée par l'article 46, il est inséré une sous-section 1re intitulée "Sous-section 1re. Certification de cybersécurité volontaire".

Art. 48

Dans la sous-section 1re, insérée par l'article 47, il est inséré un article XV.30/3, rédigé comme suit:

"Art. XV.30/3. En matière de certification de cybersécurité volontaire, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [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], à certains agents du SPF Économie, à condition que le SPF Économie dispose de l'expertise requise à ces fins. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée. Le SPF Économie exerce ces missions de contrôle uniquement sur les produits ou entités réglementés par le présent Code, ses arrêtés d'exécution ou les règlements de l'Union européenne relatifs aux matières qui, conformément aux livres VI, VII, IX et XII du présent Code, relèvent du pouvoir réglementaire du Roi."

Art. 49

Dans la section 10, insérée par l'article 46, il est inséré une sous-section 2 intitulée "Sous-section 2. Certification de cybersécurité obligatoire".

de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013."

Art. 46

In boek XV, titel 1, hoofdstuk 2, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, wordt een afdeling 10 ingevoegd, luidende "Afdeling 10. Certificering van de cyberbeveiliging".

Art. 47

In afdeling 10, ingevoegd bij artikel 46, wordt een onderafdeling 1 ingevoegd, luidende "Onderafdeling 1. Vrijwillige cyberbeveiligingscertificering".

Art. 48

In onderafdeling 1, ingevoegd bij artikel 47, wordt een artikel XV.30/3 ingevoegd, luidende:

"Art. XV. 30/3. Op het gebied van vrijwillige cyberbeveiligingscertificering kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], aan bepaalde ambtenaren van de FOD Economie toevertrouwen, op voorwaarde dat de FOD Economie over de daarvoor vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet. De FOD Economie vervult die toezichtsopdrachten enkel ten aanzien van producten of entiteiten die gereglementeerd zijn door dit Wetboek, de uitvoeringsbesluiten ervan of verordeningen van de Europese Unie betreffende aangelegenheden die, overeenkomstig de boeken VI, VII, IX en XII van dit Wetboek, tot de regelgevende bevoegdheid van de Koning behoren."

Art. 49

In afdeling 10, ingevoegd bij artikel 46, wordt een onderafdeling 2 ingevoegd, luidende "Onderafdeling 2. Verplichte cyberbeveiligingscertificering".

Art. 50

Dans la sous-section 2, insérée par l'article 49, il est inséré un article XV.30/4, rédigé comme suit:

"Art. XV.30/4. § 1er. En matière de certification européenne de cybersécurité rendue obligatoire en vertu du droit de l'Union ou du droit national, après avis de l'autorité nationale de certification de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions en matière de contrôle relatives au règlement sur la cybersécurité ou relatives à la loi du [date] 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, à certains agents du SPF Économie, à condition que ce dernier dispose de l'expertise requise à ces fins.

§ 2. Les missions en matière de contrôle visées au paragraphe 1er, y compris la recherche, la constatation, la poursuite et la sanction des infractions, s'effectuent conformément aux dispositions du présent livre."

Art. 51

Dans le livre XV, titre 3, chapitre 2, section 11/3, du même Code, insérée par la loi du 18 avril 2017, sont insérés les articles XV.125/5 et XV.125/6, rédigés comme suit:

"Art. XV.125/5. Dans le cadre de la surveillance visée à l'article [XV.30/4], sont punis d'une sanction de niveau 2:

1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "élémentaire" qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;

2° quiconque ne coopère pas lors d'un contrôle en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou ne coopère pas lors d'un contrôle de toute autre manière.

Art. XV.125/6. Dans le cadre de la surveillance visée à l'article [XV.30/4], sont punis d'une sanction de niveau 3:

1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit "substantiel" ou "élevé"

Art. 50

In onderafdeling 2, ingevoegd bij artikel 49, wordt een artikel XV.30/4 ingevoegd, luidende:

"Art. XV.30/4. § 1. Met betrekking tot de Europese cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving, na advies van de nationale cyberbeveiligingscertificeringsautoriteit, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichtsopdrachten in verband met de Cyberbeveiligingsverordening of in verband met de wet van [datum] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, toevertrouwen aan bepaalde ambtenaren van de FOD Economie, op voorwaarde dat die laatste over de voor deze doeleinden vereiste expertise beschikt.

§ 2. De in de eerste paragraaf bedoelde toezichtsopdrachten, met inbegrip van de opsporing, vaststelling, vervolging en bestraffing van inbreuken, worden uitgeoefend overeenkomstig de bepalingen van dit boek."

Art. 51

In boek XV, titel 3, hoofdstuk 2, afdeling 11/3, van hetzelfde Wetboek, ingevoegd bij de wet van 18 april 2017, worden de artikelen XV.125/5 en XV.125/6 ingevoegd, luidende:

"Art. XV.125/5. Wordt in het kader van het toezicht bedoeld in artikel [XV.30/4] gestraft met een sanctie van niveau 2:

1° de houder van een cyberbeveiligingscertificaat dat verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling;

2° eenieder die niet meewerkt tijdens een inspectie door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken of die anderszins weigert mee te werken tijdens een inspectie.

Art. XV.125/6. Wordt in het kader van het toezicht bedoeld in artikel [XV.30/4] gestraft met een sanctie van niveau 3:

1° de houder van een cyberbeveiligingscertificaat dat verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "substantieel" of "hoog"

qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;

2° quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité.".

CHAPITRE 10.

Entrée en vigueur

Art. 52

La présente loi entre en vigueur le jour de sa publication au *Moniteur belge*.

Donné à Bruxelles, le 20 mai 2022.

PHILIPPE

PAR LE ROI:

Le premier ministre,

Alexander DE CROO

Le ministre de l'Économie,

Pierre-Yves DERMAGNE

Le ministre des Finances, chargé de la Coordination de la lutte contre la fraude,

Vincent VAN PETEGHEM

La ministre des Télécommunications et de la Poste,

Petra DE SUTTER

die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken cyberbeveiligingscertificeringsregeling;

2° eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening.".

HOOFDSTUK 10

Inwerkingtreding

Art. 52

Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Gegeven te Brussel, 20 mei 2022.

FILIP

VAN KONINGSWEGE:

De eerste minister,

Alexander DE CROO

De minister van Economie,

Pierre-Yves DERMAGNE

De minister van Financiën, belast met de coördinatie van de fraudebestrijding,

Vincent VAN PETEGHEM

De minister van Telecommunicatie en Post,

Petra DE SUTTER

TABLEAU DE CORRESPONDANCE RÈGLEMENT – PROJET DE LOI

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	Projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité
	CHAPITRE 1er. - Définitions et dispositions générales
	Section 1re. - Objet et champ d'application
	Sous-section 1re. – Objet
N/A	Art. 1
N/A	Art. 2
	Sous-section 2. - Champ d'application
Art. 1, al. 1, b)	Art. 3
	Section 2. – Définitions
N/A	Art. 4
	CHAPITRE 2. - Autorités compétentes et coopération au niveau national
	Section 1re. Autorités compétentes
Art. 58, § 1er	Art. 5
	Section 2. - Coopération au niveau national
Art. 58, § 7, h)	Art. 6
N/A	Art. 7
	CHAPITRE 3. - Autorité nationale de certification de cybersécurité

	Section 1re. - Représentation au Groupe européen de certification de cybersécurité
Art. 58, § 6 ; Art. 62, § 2 et § 3	Art. 8
	Section 2. – Indépendance
Art. 58, § 3	Art. 9
	CHAPITRE 4. - Délivrance des certificats européens
	Section 1re. - Certificats de cybersécurité européens attestant d'un niveau d'assurance « élémentaire » ou « substantiel »
Art. 56, § 4 ; Art. 56, § 5	Art.10
	Section 2. - Certificats de cybersécurité européens attestant d'un niveau d'assurance « élevé »
Art. 56, § 6 ; Art. 56, § 6, b)	Art. 11
	Section 3. - Réclamation en cas de refus de délivrance
Art. 63, § 1er	Art. 12
	CHAPITRE 5. - Contrôle
Art. 58, § 4, §7 et § 8	Art. 13
Art. 58, § 9	Art. 14
Art. 58, § 3, §7 et § 8	Art. 15
Art. 58, § 7, a), c) et h)	Art. 16
Art. 58, § 7, a), c) et h)	Art. 17
Art. 53, § 3 ; 58, § 8, a)	Art. 18
	CHAPITRE 6. – Sanctions

	Section 1re. - Procédure
Art. 58, § 7, a), b), d) ; Art. 58, § 8, c), f)	Art. 19
N/A	Art. 20
	Section 2. - Retrait d'un certificat
Art. 58, § 8, e)	Art. 21
	Section 3. - Limitation, suspension ou retrait d'une autorisation ou d'une délégation
Art. 58, § 7, e)	Art. 22
	Section 4. - Amendes administratives
Art. 58, § 8, f) ; Art. 65	Art. 23
Art. 65	Art. 24
Art. 64	Art. 25
Art. 65	Art. 26
Art. 65	Art. 27
Art. 65	Art. 28
	CHAPITRE 7. – Réclamations
	Section 1re. - Saisine de l'autorité nationale de certification de cybersécurité
Art. 58 § 7, f) ; Art. 63, § 1	Art. 29
Art. 58 § 7, f) ; Art. 63, § 1	Art. 30
Art. 58 § 7, f) ; Art. 63, § 1	Art. 31
Art. 58 § 7, f) ; Art. 63, § 1	Art. 32
Art. 58 § 7, f) ; Art. 63, § 1	Art. 33

Art. 58 § 7, f) ; Art. 63, § 1	Art. 34
	Section 2. Recours
Art. 64	Art. 35
	CHAPITRE 8. - Traitement des données à caractère personnel
	Section 1. - Principes relatifs au traitement, base légale et finalités
N/A	Art. 36
N/A	Art. 37
	Section 2. - Durée de conservation
N/A	Art. 38
	CHAPITRE 9. - Dispositions modificatives
	Section 1re. - Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges
N/A	Art. 39
Art. 58, § 7, a) ; h)	Art. 40
	Section 2. - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers
N/A	Art. 41
Art. 58, § 7, a) ; h)	Art. 42
	Section 3. - Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 58, § 7, a) ; h)	Art. 43
N/A	Art. 44
	Section 4. – Modifications du Code de droit économique
N/A	Art. 45
N/A	Art. 46
N/A	Art. 47
N/A	Art. 48
N/A	Art. 49
N/A	Art. 50
Art. 65	Art. 51
	CHAPITRE 10. - Entrée en vigueur
N/A	Art. 52

CONCORDANTIETABEL VERORDENING - WETSONTWERP

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	Wetsontwerp inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit
	HOOFDSTUK 1. - Definities en algemene bepalingen
	Afdeling 1. - Onderwerp en toepassingsgebied
	Onderafdeling 1. - Onderwerp
N/A	Art. 1
N/A	Art. 2
	Onderafdeling 2. – Toepassingsgebied
Art. 1, al. 1, b)	Art. 3
	Afdeling 2. – Definities
N/A	Art. 4
	HOOFDSTUK 2. - Bevoegde autoriteiten en samenwerking op nationaal niveau
	Afdeling 1. Bevoegde autoriteiten
Art. 58, § 1er	Art. 5
	Afdeling 2. - Samenwerking op nationaal niveau
Art. 58, § 7, h)	Art. 6
N/A	Art. 7
	HOOFDSTUK 3. - Nationale cyberbeveiligingscertificeringsautoriteit
	Afdeling 1. - Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering
Art. 58, § 6 ; Art. 62, § 2 et § 3	Art. 8

	Afdeling 2. - Onafhankelijkheid
Art. 58, § 3	Art. 9
	HOOFDSTUK 4. - Afgifte van Europese certificaten
	Afdeling 1. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"
Art. 56, § 4 ; Art. 56, § 5	Art.10
	Afdeling 2. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"
Art. 56, § 6 ; Art. 56, § 6, b)	Art. 11
	Afdeling 3. - Klacht ingeval de afgifte geweigerd wordt
Art. 63, § 1er	Art. 12
	HOOFDSTUK 5. - Toezicht
Art. 58, § 4, §7 et § 8	Art. 13
Art. 58, § 9	Art. 14
Art. 58, § 3, §7 et § 8	Art. 15
Art. 58, § 7, a), c) et h)	Art. 16
Art. 58, § 7, a), c) et h)	Art. 17
Art. 53, § 3 ; 58, § 8, a)	Art. 18
	HOOFDSTUK 6. - Sancties
	Afdeling 1. - Procedure
Art. 58, § 7, a), b), d) ; Art. 58, § 8, c), f)	Art. 19
N/A	Art. 20
	Afdeling 2. - Intrekking van een certificaat
Art. 58, § 8, e)	Art. 21

	Afdeling 3. - Beperken, opschorten of intrekken van een toelating of een delegatie
Art. 58, § 7, e)	Art. 22
	Afdeling 4. - Administratieve geldboetes
Art. 58, § 8, f) ; Art. 65	Art. 23
Art. 65	Art. 24
Art. 64	Art. 25
Art. 65	Art. 26
Art. 65	Art. 27
Art. 65	Art. 28
	HOOFDSTUK 7. - Klachten
	Afdeling 1. - Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit
Art. 58 § 7, f) ; Art. 63, § 1	Art. 29
Art. 58 § 7, f) ; Art. 63, § 1	Art. 30
Art. 58 § 7, f) ; Art. 63, § 1	Art. 31
Art. 58 § 7, f) ; Art. 63, § 1	Art. 32
Art. 58 § 7, f) ; Art. 63, § 1	Art. 33
Art. 58 § 7, f) ; Art. 63, § 1	Art. 34
	Afdeling 2. Beroepen
Art. 64	Art. 35
	HOOFDSTUK 8. – Verwerking van persoonsgegevens
	Afdeling 1. – Beginselen inzake verwerking, wettelijke basis en doeleinden
N/A	Art. 36
N/A	Art. 37

	Afdeling 2. - Bewaartermijn
N/A	Art. 38
	HOOFDSTUK 9. – Wijzigingsbepalingen
	Afdeling 1. - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector
N/A	Art. 39
Art. 58, § 7, a) ; h)	Art. 40
	Afdeling 2. - Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
N/A	Art. 41
Art. 58, § 7, a) ; h)	Art. 42
	Afdeling 3. - Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België
Art. 58, § 7, a) ; h)	Art. 43
N/A	Art. 44
	Afdeling 4. - Wijzigingen van het Wetboek van economisch recht
N/A	Art. 45
N/A	Art. 46
N/A	Art. 47
N/A	Art. 48
N/A	Art. 49
N/A	Art. 50
Art. 65	Art. 51
	HOOFDSTUK 10. – Inwerkingtreding

N/A	Art. 52

TABLEAU DE CORRESPONDANCE PROJET DE LOI - RÈGLEMENT

Projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité	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
CHAPITRE 1er. - Définitions et dispositions générales	
Section 1re. - Objet et champ d'application	
Sous-section 1re. – Objet	
Art. 1	N/A
Art. 2	N/A
Sous-section 2. - Champ d'application	
Art. 3	Art. 1, al. 1, b)
Section 2. – Définitions	
Art. 4	N/A
CHAPITRE 2. - Autorités compétentes et coopération au niveau national	
Section 1re. Autorités compétentes	
Art. 5	Art. 58, § 1er
Section 2. - Coopération au niveau national	
Art. 6	Art. 58, § 7, h)
Art. 7	N/A

CHAPITRE 3. - Autorité nationale de certification de cybersécurité	
Section 1re. - Représentation au Groupe européen de certification de cybersécurité	
Art. 8	Art. 58, § 6 ; Art. 62, § 2 et § 3
Section 2. – Indépendance	
Art. 9	Art. 58, § 3
CHAPITRE 4. - Délivrance des certificats européens	
Section 1re. - Certificats de cybersécurité européens attestant d'un niveau d'assurance « élémentaire » ou « substantiel »	
Art.10	Art. 56, § 4 ; Art. 56, § 5
Section 2. - Certificats de cybersécurité européens attestant d'un niveau d'assurance « élevé »	
Art. 11	Art. 56, § 6 ; Art. 56, § 6, b)
Section 3. - Réclamation en cas de refus de délivrance	
Art. 12	Art. 63, § 1er
CHAPITRE 5. - Contrôle	
Art. 13	Art. 58, § 4, §7 et § 8
Art. 14	Art. 58, § 9
Art. 15	Art. 58, § 3, §7 et § 8
Art. 16	Art. 58, § 7, a), c) et h)
Art. 17	Art. 58, § 7, a), c) et h)

Art. 18	Art. 53, § 3 ; 58, § 8, a)
CHAPITRE 6. – Sanctions	
Section 1re. - Procédure	
Art. 19	Art. 58, § 7, a), b), d) ; Art. 58, § 8, c), f)
Art. 20	N/A
Section 2. - Retrait d'un certificat	
Art. 21	Art. 58, § 8, e)
Section 3. - Limitation, suspension ou retrait d'une autorisation ou d'une délégation	
Art. 22	Art. 58, § 7, e)
Section 4. - Amendes administratives	
Art. 23	Art. 58, § 8, f) ; Art. 65
Art. 24	Art. 65
Art. 25	Art. 64
Art. 26	Art. 65
Art. 27	Art. 65
Art. 28	Art. 65
CHAPITRE 7. – Réclamations	
Section 1re. - Saisine de l'autorité nationale de certification de cybersécurité	
Art. 29	Art. 58 § 7, f) ; Art. 63, § 1
Art. 30	Art. 58 § 7, f) ; Art. 63, § 1

Art. 31	Art. 58 § 7, f) ; Art. 63, § 1
Art. 32	Art. 58 § 7, f) ; Art. 63, § 1
Art. 33	Art. 58 § 7, f) ; Art. 63, § 1
Art. 34	Art. 58 § 7, f) ; Art. 63, § 1
Section 2. Recours	
Art. 35	Art. 64
CHAPITRE 8. - Traitement des données à caractère personnel	
Section 1. - Principes relatifs au traitement, base légale et finalités	
Art. 36	N/A
Art. 37	N/A
Section 2. - Durée de conservation	
Art. 38	N/A
CHAPITRE 9. - Dispositions modificatives	
Section 1re. - Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	
Art. 39	N/A
Art. 40	Art. 58, § 7, a) ; h)
Section 2. - Modifications de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	
Art. 41	N/A

Art. 42	Art. 58, § 7, a) ; h)
Section 3. - Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique	
Art. 43	Art. 58, § 7, a) ; h)
Art. 44	N/A
Section 4. – Modifications du Code de droit économique	
Art. 45	N/A
Art. 46	N/A
Art. 47	N/A
Art. 48	N/A
Art. 49	N/A
Art. 50	N/A
Art. 51	Art. 65
CHAPITRE 10. - Entrée en vigueur	
Art. 52	N/A

CONCORDANTIETABEL WETSONTWERP - VERORDENING

Wetsontwerp inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit	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
HOOFDSTUK 1. - Definities en algemene bepalingen	
Afdeling 1. - Onderwerp en toepassingsgebied	
Onderafdeling 1. - Onderwerp	
Art. 1	N/A
Art. 2	N/A
Onderafdeling 2. – Toepassingsgebied	
Art. 3	Art. 1, al. 1, b)
Afdeling 2. – Definities	
Art. 4	N/A
HOOFDSTUK 2. - Bevoegde autoriteiten en samenwerking op nationaal niveau	
Afdeling 1. Bevoegde autoriteiten	
Art. 5	Art. 58, § 1er
Afdeling 2. - Samenwerking op nationaal niveau	
Art. 6	Art. 58, § 7, h)
Art. 7	N/A
HOOFDSTUK 3. - Nationale cyberbeveiligingscertificeringsautoriteit	
Afdeling 1. - Vertegenwoordiging in de Europese Groep voor cyberbeveiligingscertificering	
Art. 8	Art. 58, § 6 ; Art. 62, § 2 et § 3

Afdeling 2. - Onafhankelijkheid	
Art. 9	Art. 58, § 3
HOOFDSTUK 4. - Afgifte van Europese certificaten	
Afdeling 1. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "basis" of "substantieel"	
Art.10	Art. 56, § 4 ; Art. 56, § 5
Afdeling 2. - Europese cyberbeveiligingscertificaten voor zekerheidsniveau "hoog"	
Art. 11	Art. 56, § 6 ; Art. 56, § 6, b)
Afdeling 3. - Klacht ingeval de afgifte geweigerd wordt	
Art. 12	Art. 63, § 1er
HOOFDSTUK 5. - Toezicht	
Art. 13	Art. 58, § 4, §7 et § 8
Art. 14	Art. 58, § 9
Art. 15	Art. 58, § 3, §7 et § 8
Art. 16	Art. 58, § 7, a), c) et h)
Art. 17	Art. 58, § 7, a), c) et h)
Art. 18	Art. 53, § 3 ; 58, § 8, a)
HOOFDSTUK 6. - Sancties	
Afdeling 1. - Procedure	
Art. 19	Art. 58, § 7, a), b), d) ; Art. 58, § 8, c), f)
Art. 20	N/A
Afdeling 2. - Intrekking van een certificaat	
Art. 21	Art. 58, § 8, e)

Afdeling 3. - Beperken, opschorten of intrekken van een toelating of een delegatie	
Art. 22	Art. 58, § 7, e)
Afdeling 4. - Administratieve geldboetes	
Art. 23	Art. 58, § 8, f) ; Art. 65
Art. 24	Art. 65
Art. 25	Art. 64
Art. 26	Art. 65
Art. 27	Art. 65
Art. 28	Art. 65
HOOFDSTUK 7. - Klachten	
Afdeling 1. - Aanhangigmaking bij de nationale cyberbeveiligingscertificeringsautoriteit	
Art. 29	Art. 58 § 7, f) ; Art. 63, § 1
Art. 30	Art. 58 § 7, f) ; Art. 63, § 1
Art. 31	Art. 58 § 7, f) ; Art. 63, § 1
Art. 32	Art. 58 § 7, f) ; Art. 63, § 1
Art. 33	Art. 58 § 7, f) ; Art. 63, § 1
Art. 34	Art. 58 § 7, f) ; Art. 63, § 1
Afdeling 2. Beroepen	
Art. 35	Art. 64
HOOFDSTUK 8. – Verwerking van persoonsgegevens	
Afdeling 1. – Beginselen inzake verwerking, wettelijke basis en doeleinden	
Art. 36	N/A
Art. 37	N/A

Afdeling 2. - Bewaartermijn	
Art. 38	N/A
HOOFDSTUK 9. – Wijzigingsbepalingen	
Afdeling 1. - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector	
Art. 39	N/A
Art. 40	Art. 58, § 7, a) ; h)
Afdeling 2. - Wijzigingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten	
Art. 41	N/A
Art. 42	Art. 58, § 7, a) ; h)
Afdeling 3. - Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België	
Art. 43	Art. 58, § 7, a) ; h)
Art. 44	N/A
Afdeling 4. - Wijzigingen van het Wetboek van economisch recht	
Art. 45	N/A
Art. 46	N/A
Art. 47	N/A
Art. 48	N/A
Art. 49	N/A
Art. 50	N/A
Art. 51	Art. 65
HOOFDSTUK 10. – Inwerkingtreding	

Art. 52	N/A

COORDINATION DES ARTICLES

Texte de base	Texte de base adapté au projet
Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges	**Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**
(…)	(…)
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 7 avril 2019 établissant un cadre pour la sécurité 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, 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:	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 7 avril 2019 établissant un cadre pour la sécurité 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, 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 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 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 Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;	b) le Titre Ier, 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;	c) la loi du 26 janvier 2018 relative aux services postaux;

d) les articles 14, § 2, 2°, 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°, 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 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;
h) 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, en ce qui concerne le secteur des infrastructures numériques;	h) 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, en ce qui concerne le secteur des infrastructures numériques;
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;	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;	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.	iii) la Commission européenne dans le secteur des communications électroniques ou dans le secteur postal.
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.	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.
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 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 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, 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'Etat 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 en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion.	6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat 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 en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion.
	7° L'Institut exerce les 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 [date] [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].
§ 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 électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte;	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;
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 et à l'ORECE;	a) la Commission européenne, l'ENISA, l'Office et à l'ORECE;
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'Economie 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'Economie 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, 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 chargé des statistiques et de l'information économique;	i) le Service public fédéral chargé des statistiques et de l'information économique;
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;

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 à la qualité et à la pérennité du service universel;
- veiller aux intérêts des utilisateurs des services postaux;	- veiller aux intérêts des utilisateurs des services postaux;
- contribuer au développement d'un marché intérieur des services postaux;	- contribuer au développement d'un marché intérieur des services postaux;
- promouvoir la concurrence dans le secteur postal;	- 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.	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.

§ 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.
(…)	(…)
Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers	**Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**
(…)	(…)
Art. 45. § 1er. La FSMA a pour mission, conformément à la présente loi et aux lois particulières qui lui sont applicables:	Art. 45. § 1er. La FSMA a pour mission, conformément à la présente loi et aux lois particulières qui lui sont applicables:
1° de veiller au respect des règles visant la protection des intérêts des investisseurs lors des transactions effectuées sur des instruments financiers et d'autres instruments de placement, ainsi qu'au respect des règles visant à garantir le bon fonctionnement, l'intégrité et la transparence des marchés d'instruments financiers et d'autres instruments de placement et, en particulier, des règles visées au chapitre II, des dispositions de la loi du 21 novembre 2017 relative aux infrastructures des marchés financiers et portant transposition de la directive 2014/65/UE, ainsi que des arrêtés et règlements pris pour l'exécution de tout ce qui précède;	1° de veiller au respect des règles visant la protection des intérêts des investisseurs lors des transactions effectuées sur des instruments financiers et d'autres instruments de placement, ainsi qu'au respect des règles visant à garantir le bon fonctionnement, l'intégrité et la transparence des marchés d'instruments financiers et d'autres instruments de placement et, en particulier, des règles visées au chapitre II, des dispositions de la loi du 21 novembre 2017 relative aux infrastructures des marchés financiers et portant transposition de la directive 2014/65/UE, ainsi que des arrêtés et règlements pris pour l'exécution de tout ce qui précède;
2° d'assurer le contrôle:	2° d'assurer le contrôle:
a. des sociétés de gestion de portefeuille et de conseil en investissement visées par la loi du 25 octobre 2016, des sociétés de gestion d'organismes de placement collectif, des gestionnaires d'OPCA visés par la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires, et des bureaux de change visés par la loi du 25 octobre 2016 et ses arrêtés d'exécution;	a. des sociétés de gestion de portefeuille et de conseil en investissement visées par la loi du 25 octobre 2016, des sociétés de gestion d'organismes de placement collectif, des gestionnaires d'OPCA visés par la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires, et des bureaux de change visés par la loi du 25 octobre 2016 et ses arrêtés d'exécution;
b. des organismes de placement collectif visés par la loi du 3 août 2012 relative aux organismes	b. des organismes de placement collectif visés par la loi du 3 août 2012 relative aux organismes

de placement collectif qui répondent aux conditions de la directive 2009/65/CE et aux organismes de placement en créances et par la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires;	de placement collectif qui répondent aux conditions de la directive 2009/65/CE et aux organismes de placement en créances et par la loi du 19 avril 2014 relative aux organismes de placement collectif alternatifs et à leurs gestionnaires;
c. [...];	c. [...];
d. des entreprises et des opérations visées par la loi du 12 juin 1991 relative au crédit à la consommation;	d. des entreprises et des opérations visées par la loi du 12 juin 1991 relative au crédit à la consommation;
[...]	[...]
e. des intermédiaires d'assurances et de réassurances visés par la loi du 4 avril 2014 relative aux assurances;	e. des intermédiaires d'assurances et de réassurances visés par la loi du 4 avril 2014 relative aux assurances;
f. des intermédiaires en services bancaires et en services d'investissement visés par la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments financiers;	f. des intermédiaires en services bancaires et en services d'investissement visés par la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments financiers;
g. [...]	g. [...]
h. des sociétés immobilières réglementées visées par la loi du 12 mai 2014 relative aux sociétés immobilières réglementées;	h. des sociétés immobilières réglementées visées par la loi du 12 mai 2014 relative aux sociétés immobilières réglementées;
i. des planificateurs financiers indépendants visés par la loi du 25 avril 2014 relative au statut et au contrôle des planificateurs financiers indépendants et à la fourniture de consultations en planification financière par des entreprises réglementées;	i. des planificateurs financiers indépendants visés par la loi du 25 avril 2014 relative au statut et au contrôle des planificateurs financiers indépendants et à la fourniture de consultations en planification financière par des entreprises réglementées;
j. des prêteurs et des intermédiaires de crédit visés au livre VII, titre 4, chapitre 4 du Code de droit économique.	j. des prêteurs et des intermédiaires de crédit visés au livre VII, titre 4, chapitre 4 du Code de droit économique.
k. des prestataires de services de financement participatif visés par le règlement (UE) 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937;	k. des prestataires de services de financement participatif visés par le règlement (UE) 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937;

l. les prestataires de services de communication de données visés par la loi du 21 novembre 2017 et portant la transposition de la Directive 2014/65/EU;	l. les prestataires de services de communication de données visés par la loi du 21 novembre 2017 et portant la transposition de la Directive 2014/65/EU;
m. des administrateurs d'indices de référence visés par le Règlement (UE) 2016/1011;	m. des administrateurs d'indices de référence visés par le Règlement (UE) 2016/1011;
n. des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation visés à l'article 5, § 1er, alinéa 1er, 14° /1 et 14° /2, 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 et à l'arrêté pris en exécution de l'article 5, § 1er, alinéa 2 de la même loi.	n. des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation visés à l'article 5, § 1er, alinéa 1er, 14° /1 et 14° /2, 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 et à l'arrêté pris en exécution de l'article 5, § 1er, alinéa 2 de la même loi.
3° de veiller au respect par les établissements de crédit, les entreprises d'assurances, les entreprises de réassurance, les sociétés de bourse, les contreparties centrales, les référentiels centraux, les dépositaires centraux de titres, les organismes de support des dépositaires centraux de titres et les banques dépositaires, et pour autant qu'elles leur soient applicables, des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:	3° de veiller au respect par les établissements de crédit, les entreprises d'assurances, les entreprises de réassurance, les sociétés de bourse, les contreparties centrales, les référentiels centraux, les dépositaires centraux de titres, les organismes de support des dépositaires centraux de titres et les banques dépositaires, et pour autant qu'elles leur soient applicables, des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:
a. les règles visées au chapitre II;	a. les règles visées au chapitre II;
b. la loi du 25 juin 1992 sur le contrat d'assurance terrestre;	b. la loi du 25 juin 1992 sur le contrat d'assurance terrestre;
c. la loi du 4 avril 2014 relative aux assurances;	c. la loi du 4 avril 2014 relative aux assurances;
d. la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments financiers;	d. la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments financiers;
e. [...];	e. [...];
f. l'article 42 de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, les articles 21, 41 à 42/2, 64, 65, § 3, 65/2 et 65/3, ainsi que l'article 66 en ce qui concerne la fourniture de services d'investissement et l'exercice d'activités d'investissement, de la loi du 25 avril 2014, les	f. l'article 42 de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, les articles 21, 41 à 42/2, 64, 65, § 3, 65/2 et 65/3, ainsi que l'article 66 en ce qui concerne la fourniture de services d'investissement et l'exercice d'activités d'investissement, de la loi du 25 avril 2014, les

articles 502, 510, 510/1, 510/2, 527, 528, 529/1, ainsi que l'article 530 en ce qui concerne la fourniture de services d'investissement et l'exercice d'activités d'investissement, de la même loi, dans la mesure où les articles 502 et 528, alinéa 1er, de cette loi rendent les articles 21 et 65, § 3, précités applicables aux sociétés de bourse, sous l'angle du respect des règles destinées à assurer un traitement honnête, équitable et professionnel des parties intéressées;	articles 502, 510, 510/1, 510/2, 527, 528, 529/1, ainsi que l'article 530 en ce qui concerne la fourniture de services d'investissement et l'exercice d'activités d'investissement, de la même loi, dans la mesure où les articles 502 et 528, alinéa 1er, de cette loi rendent les articles 21 et 65, § 3, précités applicables aux sociétés de bourse, sous l'angle du respect des règles destinées à assurer un traitement honnête, équitable et professionnel des parties intéressées;
g. les articles 65, §§ 1er et 2, et 528, alinéa 1er de la loi du 25 avril 2014, dans la mesure où ce dernier article rend l'article 65, §§ 1er et 2, précité applicable aux sociétés de bourse;	g. les articles 65, §§ 1er et 2, et 528, alinéa 1er de la loi du 25 avril 2014, dans la mesure où ce dernier article rend l'article 65, §§ 1er et 2, précité applicable aux sociétés de bourse;
h) les dispositions visées à l'article 16, § 7, de la loi du 13 novembre 2011 relative à l'indemnisation des dommages corporels et moraux découlant d'un accident technologique;	h) les dispositions visées à l'article 16, § 7, de la loi du 13 novembre 2011 relative à l'indemnisation des dommages corporels et moraux découlant d'un accident technologique;
i. la loi du 25 avril 2014 relative au statut et au contrôle des planificateurs financiers indépendants et à la fourniture de consultations en planification financière par des entreprises réglementées;	i. la loi du 25 avril 2014 relative au statut et au contrôle des planificateurs financiers indépendants et à la fourniture de consultations en planification financière par des entreprises réglementées;
j. L'article 383 de la loi du 25 avril 2014;	j. L'article 383 de la loi du 25 avril 2014;
k. Titre II de la loi du 18 décembre 2016 organisant la reconnaissance et l'encadrement du crowdfunding et portant des dispositions diverses en matière de finances;	k. Titre II de la loi du 18 décembre 2016 organisant la reconnaissance et l'encadrement du crowdfunding et portant des dispositions diverses en matière de finances;
4° de veiller au respect des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:	4° de veiller au respect des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:
a. le titre II, chapitre 1er, section 4, de la loi-programme (I) du 24 décembre 2002, relatif à la pension complémentaire pour indépendants;	a. le titre II, chapitre 1er, section 4, de la loi-programme (I) du 24 décembre 2002, relatif à la pension complémentaire pour indépendants;
b. la loi du 28 avril 2003 relative aux pensions complémentaires et au régime fiscal de celles-ci et de certains avantages complémentaires en matière de sécurité sociale;	b. la loi du 28 avril 2003 relative aux pensions complémentaires et au régime fiscal de celles-ci et de certains avantages complémentaires en matière de sécurité sociale;
c. le titre 4 de la loi du 15 mai 2014 portant des dispositions diverses, relatif à la pension complémentaire pour dirigeants d'entreprise;	c. le titre 4 de la loi du 15 mai 2014 portant des dispositions diverses, relatif à la pension complémentaire pour dirigeants d'entreprise;

d. le titre II de la loi du 18 février 2018 portant des dispositions diverses en matière de pensions complémentaires et instaurant une pension complémentaire pour les travailleurs indépendants personnes physiques, pour les conjoints aidants et pour les aidants indépendants;	d. le titre II de la loi du 18 février 2018 portant des dispositions diverses en matière de pensions complémentaires et instaurant une pension complémentaire pour les travailleurs indépendants personnes physiques, pour les conjoints aidants et pour les aidants indépendants;
e. le titre 2 de la loi du 6 décembre 2018 instaurant une pension libre complémentaire pour les travailleurs salariés et portant des dispositions diverses en matière de pensions complémentaires;	e. le titre 2 de la loi du 6 décembre 2018 instaurant une pension libre complémentaire pour les travailleurs salariés et portant des dispositions diverses en matière de pensions complémentaires;
e. l'article 12 de la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, dans la mesure où l'article 32 de cette loi prévoit la compétence de la FSMA, et l'article 12 de la loi du 10 mai 2007 tendant à lutter contre la discrimination entre les femmes et les hommes, dans la mesure où l'article 38 de cette loi prévoit la compétence de la FSMA;	e. l'article 12 de la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, dans la mesure où l'article 32 de cette loi prévoit la compétence de la FSMA, et l'article 12 de la loi du 10 mai 2007 tendant à lutter contre la discrimination entre les femmes et les hommes, dans la mesure où l'article 38 de cette loi prévoit la compétence de la FSMA;
4° /1 de veiller au respect des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:	4° /1 de veiller au respect des dispositions suivantes et des arrêtés et règlements pris pour leur exécution:
a. les dispositions visées à l'article 15, alinéa 1er, de la loi du 21 décembre 2013 relative à diverses dispositions concernant le financement des petites et moyennes entreprises;	a. les dispositions visées à l'article 15, alinéa 1er, de la loi du 21 décembre 2013 relative à diverses dispositions concernant le financement des petites et moyennes entreprises;
b. les dispositions visées à l'article 17, § 1er, de la loi du 26 décembre 2013 portant diverses dispositions concernant les prêts-citoyen thématiques;	b. les dispositions visées à l'article 17, § 1er, de la loi du 26 décembre 2013 portant diverses dispositions concernant les prêts-citoyen thématiques;
5° de contribuer au respect des règles visant à protéger les utilisateurs de produits ou services financiers et les emprunteurs contre l'offre ou la fourniture illicite de produits ou services financiers et contre l'usage illégal de dénominations réservées à des entreprises agréées, inscrites ou enregistrées auprès de la FSMA ou de la Banque;	5° de contribuer au respect des règles visant à protéger les utilisateurs de produits ou services financiers et les emprunteurs contre l'offre ou la fourniture illicite de produits ou services financiers et contre l'usage illégal de dénominations réservées à des entreprises agréées, inscrites ou enregistrées auprès de la FSMA ou de la Banque;
6° de contribuer à l'éducation financière;	6° de contribuer à l'éducation financière;
7° de contribuer au respect des dispositions du livre VI du Code de droit économique et des	7° de contribuer au respect des dispositions du livre VI du Code de droit économique et des

arrêtés et règlements pris pour leur exécution, qui ont trait aux services financiers tels que visés au livre Ier du même Code, par les entreprises soumises à son contrôle ou dont les opérations ou produits sont soumis à son contrôle.	arrêtés et règlements pris pour leur exécution, qui ont trait aux services financiers tels que visés au livre Ier du même Code, par les entreprises soumises à son contrôle ou dont les opérations ou produits sont soumis à son contrôle.
Sur avis de la Banque et de la FSMA, le Roi, afin de tenir compte, notamment, de l'état de la réglementation européenne en la matière, peut, pour l'exécution des dispositions visées à l'alinéa 1er, 3°, et pour le contrôle par la FSMA du respect de celles-ci par les institutions ou personnes visées à l'alinéa 1er, 2° ou 3°, opérer une distinction entre les parties intéressées professionnelles et les parties intéressées de détail ou entre certaines catégories de parties intéressées professionnelles.	Sur avis de la Banque et de la FSMA, le Roi, afin de tenir compte, notamment, de l'état de la réglementation européenne en la matière, peut, pour l'exécution des dispositions visées à l'alinéa 1er, 3°, et pour le contrôle par la FSMA du respect de celles-ci par les institutions ou personnes visées à l'alinéa 1er, 2° ou 3°, opérer une distinction entre les parties intéressées professionnelles et les parties intéressées de détail ou entre certaines catégories de parties intéressées professionnelles.
Par dérogation à l'alinéa 1er, le contrôle du respect des règles visées à l'alinéa 1er, 3°, et au § 2, par les sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités relève des compétences de l'Office de contrôle des mutualités et des unions nationales de mutualités.	Par dérogation à l'alinéa 1er, le contrôle du respect des règles visées à l'alinéa 1er, 3°, et au § 2, par les sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités relève des compétences de l'Office de contrôle des mutualités et des unions nationales de mutualités.
La FSMA a également pour mission, dans la mesure définie par 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, de contrôler le respect, par les entités assujetties visées à l'article 85, § 1er, 4°, de la même loi, des dispositions légales et réglementaires ou de droit européen qui ont pour objet la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, ainsi que du financement de la prolifération des armes de destruction massive.	La FSMA a également pour mission, dans la mesure définie par 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, de contrôler le respect, par les entités assujetties visées à l'article 85, § 1er, 4°, de la même loi, des dispositions légales et réglementaires ou de droit européen qui ont pour objet la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, ainsi que du financement de la prolifération des armes de destruction massive.
§ 2. Afin de promouvoir le traitement honnête, équitable et professionnel des parties intéressées, le Roi peut, sur avis de la FSMA et de la Banque, compléter à l'égard des institutions ou personnes visées au § 1er, alinéa 1er, 2° et 3°, les règles visées au § 1er, alinéa 1er, 3°, par des dispositions concernant:	§ 2. Afin de promouvoir le traitement honnête, équitable et professionnel des parties intéressées, le Roi peut, sur avis de la FSMA et de la Banque, compléter à l'égard des institutions ou personnes visées au § 1er, alinéa 1er, 2° et 3°, les règles visées au § 1er, alinéa 1er, 3°, par des dispositions concernant:

- les obligations d'information à l'égard des parties intéressées;	- les obligations d'information à l'égard des parties intéressées;
- les obligations et les conditions contractuelles;	- les obligations et les conditions contractuelles;
- l'obligation de servir au mieux les intérêts des clients (devoir de diligence);	- l'obligation de servir au mieux les intérêts des clients (devoir de diligence);
- les régimes relatifs aux avantages liés aux services prestés;	- les régimes relatifs aux avantages liés aux services prestés;
- la fourniture de services via Internet;	- la fourniture de services via Internet;
- les règles de publicité;	- les règles de publicité;
- le traitement des plaintes;	- le traitement des plaintes;
- la transparence, par la mention obligatoire d'un label ou de toute autre façon, des risques, des prix, des rémunérations et des frais;	- la transparence, par la mention obligatoire d'un label ou de toute autre façon, des risques, des prix, des rémunérations et des frais;
- l'accessibilité aux services fournis.	- l'accessibilité aux services fournis.
Il peut, en particulier, prévoir des règles différentes selon qu'il s'agit de parties intéressées professionnelles ou de parties intéressées de détail, ou des règles différentes entre certaines catégories de parties intéressées professionnelles.	Il peut, en particulier, prévoir des règles différentes selon qu'il s'agit de parties intéressées professionnelles ou de parties intéressées de détail, ou des règles différentes entre certaines catégories de parties intéressées professionnelles.
§ 3. Pour l'application du présent article, il y a lieu d'entendre par " parties intéressées " les clients et les clients potentiels des entreprises concernées, ainsi que les preneurs d'assurance, les assurés et les bénéficiaires des contrats d'assurance souscrits auprès des entreprises d'assurances.	§ 3. Pour l'application du présent article, il y a lieu d'entendre par " parties intéressées " les clients et les clients potentiels des entreprises concernées, ainsi que les preneurs d'assurance, les assurés et les bénéficiaires des contrats d'assurance souscrits auprès des entreprises d'assurances.
§ 4. Les dispositions des articles 36 et 37 sont applicables en cas de non-respect des règles visées au § 1er, alinéa 1er, 3°, f et g, ou de manquement aux obligations prévues en vertu du paragraphe 2.	§ 4. Les dispositions des articles 36 et 37 sont applicables en cas de non-respect des règles visées au § 1er, alinéa 1er, 3°, f et g, ou de manquement aux obligations prévues en vertu du paragraphe 2.
§ 5. Dans l'exercice de ses fonctions, la FSMA, en sa qualité d'autorité prudentielle compétente, tient compte de la convergence, en matière d'outils de surveillance et de pratiques de surveillance, de l'application des obligations législatives, réglementaires et administratives	§ 5. Dans l'exercice de ses fonctions, la FSMA, en sa qualité d'autorité prudentielle compétente, tient compte de la convergence, en matière d'outils de surveillance et de pratiques de surveillance, de l'application des obligations législatives, réglementaires et administratives

imposées conformément aux directives européennes applicables.	imposées conformément aux directives européennes applicables.
Elle doit, à cet effet:	Elle doit, à cet effet:
a) participer aux activités de l'Autorité bancaire européenne;	a) participer aux activités de l'Autorité bancaire européenne;
b) se conformer aux lignes directrices, aux recommandations, aux normes et aux autres mesures convenues par l'Autorité bancaire européenne et, si elle ne le fait pas, en donner les raisons.	b) se conformer aux lignes directrices, aux recommandations, aux normes et aux autres mesures convenues par l'Autorité bancaire européenne et, si elle ne le fait pas, en donner les raisons.
Dans l'exercice de ses missions générales, la FSMA, en sa qualité d'autorité prudentielle compétente, tient dûment compte de l'impact potentiel de ses décisions sur la stabilité du système financier dans tous les autres Etats membres concernés et, en particulier, dans les situations d'urgence, en se fondant sur les informations disponibles au moment considéré.	Dans l'exercice de ses missions générales, la FSMA, en sa qualité d'autorité prudentielle compétente, tient dûment compte de l'impact potentiel de ses décisions sur la stabilité du système financier dans tous les autres Etats membres concernés et, en particulier, dans les situations d'urgence, en se fondant sur les informations disponibles au moment considéré.
	§ 6. A la demande de la FSMA et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la FSMA, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée et la FSMA. La FSMA exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu du paragraphe 1er, 2°, du présent article et des lois particulières qui régissent le contrôle des établissements financiers.
(…)	(…)
Art. 75. § 1er. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles:	Art. 75. § 1er. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles:

1° à la Banque centrale européenne, à la Banque 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, à la Banque 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 Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA 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 Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA 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 FSMA peut divulguer, dans tous les Etats 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 FSMA peut divulguer, dans tous les Etats 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;
1° bis à la Banque;, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en	1° bis à la Banque;, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en

matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC;	matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC;
2° à l'Agence Fédérale de la Dette;	2° à l'Agence Fédérale de la Dette;
3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45;	3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45;
4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations;	4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations;
5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement;	5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement;
6° 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;	6° 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;
7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;	7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné;
8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent;	8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent;
9° 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	9° 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 entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;	des entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures;
10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères;	10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères;
11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA;	11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA;
12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA;	12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA;
13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, *et pour le contrôle relatif au crédit hypothécaire* aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations;	13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, *et pour le contrôle relatif au crédit hypothécaire* aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations;
14° à l'Autorité belge de la concurrence;	14° à l'Autorité belge de la concurrence;
15° les autorités visées à l'article 7 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 pour les besoins de l'exécution des dispositions de cette loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;	15° les autorités visées à l'article 7 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 pour les besoins de l'exécution des dispositions de cette loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;
16° à l'Administration générale de la Trésorerie du Service fédéral Finances lorsqu'une telle	16° à l'Administration générale de la Trésorerie du Service 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 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces) 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;	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 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces) 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;
17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuaires;	17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuaires;
18° à Fedris;	18° à Fedris;
19° à l'Office de contrôle des mutualités et des unions nationales de mutualités, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités, ainsi que de leurs opérations.	19° à l'Office de contrôle des mutualités et des unions nationales de mutualités, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités, ainsi que de leurs opérations.
20° [...]	20° [...]
21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique.	21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique.
22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission;	22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission;
23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles;	23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles;
24° à l'Autorité belge de protection des données;	24° à l'Autorité belge de protection des données;
24° à la Cellule de traitement des informations financières, visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du	24° à la Cellule de traitement des informations financières, visée à l'article 76 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;	blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;
25° au cours de procédures de liquidation d'une institution de retraite professionnelle ou d'un régime de retraite au sens de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle, aux autorités et personnes impliquées dans ces procédures, ainsi qu'aux autorités chargées de la surveillance de ces autorités ou personnes;	25° au cours de procédures de liquidation d'une institution de retraite professionnelle ou d'un régime de retraite au sens de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle, aux autorités et personnes impliquées dans ces procédures, ainsi qu'aux autorités chargées de la surveillance de ces autorités ou personnes;
26° aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 38 du règlement 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937, ainsi qu'aux prestataires de services de financement participatif, dans la mesure nécessaire pour le traitement de ladite réclamation.	26° aux personnes ayant introduit une réclamation auprès de la FSMA, en application de l'article 38 du règlement 2020/1503 du Parlement européen et du Conseil du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs, et modifiant le règlement (UE) 2017/1129 et la directive (UE) 2019/1937, ainsi qu'aux prestataires de services de financement participatif, dans la mesure nécessaire pour le traitement de ladite réclamation.
	27° à l'autorité visée à l'article 5, § 1er, de la loi du […] 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.
(…)	(…)
Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique	**Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**
(…)	(…)
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:	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:
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	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.	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 Etats 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 et des sociétés de bourse 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 Etats 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 et des sociétés de bourse 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 Etats 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 Etats 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 Etats 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 Etats 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 Etats 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 Etats 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'Etats 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'Etats 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 (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010;	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;
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 visée à l'article 7, § 1er, de la loi du 7 avril 2019 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 visée à l'article 7, § 1er, de la loi du 7 avril 2019 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° /1 dans les limites du droit de l'Union européenne, aux services de police et à l'autorité visée à l'article 7, § 1er, 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 - loi NIS 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 visée à l'article 7, § 1er, 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 - loi NIS 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 […] 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 contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43bis, § 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;	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 43bis, § 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 Etats 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 Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action 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 et des sociétés de bourse;	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 et des sociétés de bourse;
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 des sociétés de bourse; et	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 des sociétés de bourse; et
c) le commissaire spécial visé à l'article 236, § 1er, 1°, de la loi précitée, à l'article 517, § 1er, 1°, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 35, § 1er, alinéa 2, 1°, de la loi du 21 décembre 2009 relative au statut des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement, l'article 87, § 1er, alinéa 2, 1°, de la loi précitée, l'article 48, alinéa 1er, 1°, 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, 3°, de la présente loi.	c) le commissaire spécial visé à l'article 236, § 1er, 1°, de la loi précitée, à l'article 517, § 1er, 1°, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 35, § 1er, alinéa 2, 1°, de la loi du 21 décembre 2009 relative au statut des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement, l'article 87, § 1er, alinéa 2, 1°, de la loi précitée, l'article 48, alinéa 1er, 1°, 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, 3°, de la présente loi.
24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019 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 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques;
25° au Service Public Fédéral Economie, P.M.E., Classes moyennes et Energie 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 Economie, P.M.E., Classes moyennes et Energie 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.
(…)	(…)
CHAPITRE IV/4. - Missions spécifiques de la Banque concernant la prévention et la gestion de crises et de risques dans le secteur financier.	**CHAPITRE IV/4. - Missions spécifiques de la Banque concernant la prévention et la gestion de crises et de risques dans le secteur financier.**
(…)	(…)
Art. 36/48. La Banque exerce les missions qui lui sont dévolues en tant qu'autorité sectorielle pour le secteur des finances en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.	Art. 36/48. La Banque exerce les missions qui lui sont dévolues en tant qu'autorité sectorielle pour le secteur des finances en vertu de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.
	Art. 36/48/1. A la demande de la Banque et en fonction de l'objet du schéma de certification de cybersécurité concerné, le Roi peut, à condition qu'elle dispose de l'expertise requise à ces fins, confier à la Banque, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité]. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée et la Banque. La Banque exerce ces missions de contrôle uniquement vis-à-vis des entités sur lesquelles elle exerce le contrôle en vertu des articles 8 et 12bis et des lois particulières qui régissent le contrôle des établissements financiers.
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	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.	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.
(…)	(…)
Code de droit économique	**Code de droit économique**
(…)	(…)
Art. I.20. Les définitions suivantes sont applicables au livre XV:	Art. I.20. Les définitions suivantes sont applicables au livre XV:
1° données à caractère personnel: informations concernant une personne physique identifiée ou identifiable, conformément à la définition prévue à l'article 1er, § 1er, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;	1° données à caractère personnel: informations concernant une personne physique identifiée ou identifiable, conformément à la définition prévue à l'article 1er, § 1er, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;
2° responsable du traitement: personne physique ou morale, association de fait ou administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;	2° responsable du traitement: personne physique ou morale, association de fait ou administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;
3° traitement: toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel;	3° traitement: toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel;
4° coordinateur fédéral: la personne physique désignée au sein du Service public fédéral Economie, pour être, dans le cadre de la coopération administrative prévue aux articles XV.35 à XV.48, le point de contact entre la Commission européenne et les autorités belges compétentes;	4° coordinateur fédéral: la personne physique désignée au sein du Service public fédéral Economie, pour être, dans le cadre de la coopération administrative prévue aux articles XV.35 à XV.48, le point de contact entre la Commission européenne et les autorités belges compétentes;
5° coordinateur d'alerte: la personne ou les personnes physiques désignées au niveau	5° coordinateur d'alerte: la personne ou les personnes physiques désignées au niveau

fédéral qui sont chargées d'assurer l'information des Etats membres et de la Commission européenne de circonstances ou de faits graves et précis en rapport avec une activité de service susceptibles de causer un préjudice grave à la santé ou à la sécurité des personnes ou à l'environnement;	fédéral qui sont chargées d'assurer l'information des Etats membres et de la Commission européenne de circonstances ou de faits graves et précis en rapport avec une activité de service susceptibles de causer un préjudice grave à la santé ou à la sécurité des personnes ou à l'environnement;
6° Banque: la Banque nationale de Belgique;	6° Banque: la Banque nationale de Belgique;
7° entreprise: toute personne physique ou personne morale poursuivant de manière durable un but économique, y compris ses associations;	7° entreprise: toute personne physique ou personne morale poursuivant de manière durable un but économique, y compris ses associations;
8° entreprise soumise à inscription: toute entité tenue de s'inscrire en vertu de l'article III.49;	8° entreprise soumise à inscription: toute entité tenue de s'inscrire en vertu de l'article III.49;
9° plaignant de la chaîne d'approvisionnement agricole et alimentaire: tout fournisseur de produits agricoles et alimentaires, toute organisation de producteurs, toute organisation de fournisseurs, toute organisation dont un producteur ou un fournisseur est membre, toute association d'organisations dont un fournisseur est membre et toute autre organisation ayant un intérêt légitime à représenter les fournisseurs pour autant qu'il s'agisse d'une personne morale indépendante sans but lucratif, qui est confronté à un acheteur de produits agricoles et alimentaires soupçonné de commettre une infraction aux dispositions visées à l'article XV.83, 15° /1.	9° plaignant de la chaîne d'approvisionnement agricole et alimentaire: tout fournisseur de produits agricoles et alimentaires, toute organisation de producteurs, toute organisation de fournisseurs, toute organisation dont un producteur ou un fournisseur est membre, toute association d'organisations dont un fournisseur est membre et toute autre organisation ayant un intérêt légitime à représenter les fournisseurs pour autant qu'il s'agisse d'une personne morale indépendante sans but lucratif, qui est confronté à un acheteur de produits agricoles et alimentaires soupçonné de commettre une infraction aux dispositions visées à l'article XV.83, 15° /1.
	10° Règlement sur la cybersécurité: 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.
(…)	(…)
Livre XV. - Application de la loi	**Livre XV. - Application de la loi**
TITRE 1er. - L'exercice de la surveillance et la recherche et la constatation des infractions	**TITRE 1er. - L'exercice de la surveillance et la recherche et la constatation des infractions**

(…)	(…)
CHAPITRE 2. - Compétences particulières	**CHAPITRE 2. - Compétences particulières**
(…)	(…)
Section 9. Autres compétences particulières	**Section 9. Autres compétences particulières**
Art. XV.30/2. Les agents désignés par le ministre sont compétents pour prêter l'assistance nécessaire aux contrôleurs de la Commission européenne, conformément à l'article 9 du règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités.	Art. XV.30/2. Les agents désignés par le ministre sont compétents pour prêter l'assistance nécessaire aux contrôleurs de la Commission européenne, conformément à l'article 9 du règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités.
Les agents visés à l'alinéa 1er disposent pour cela des compétences prévues au titre 1er, chapitre 1er.	Les agents visés à l'alinéa 1er disposent pour cela des compétences prévues au titre 1er, chapitre 1er.
	Section 10. Certification de cybersécurité
	Sous-section 1ère. Certification de cybersécurité volontaire
	Art. XV.30/3. En matière de certification de cybersécurité volontaire, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions visées aux chapitres 5 et 6, à l'exception des articles 21 et 22, de la loi du [date] [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], à certains agents du SPF Economie, à condition que le SPF Economie dispose de l'expertise requise à ces fins. Dans cette hypothèse, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée à l'article 5, § 1er, de la loi précitée. Le SPF Economie exerce ces missions de contrôle uniquement sur les produits ou entités réglementés par le présent Code, ses arrêtés d'exécution ou les règlements de l'Union européenne relatifs aux matières qui,

	conformément aux livres VI, VII, IX et XII du présent Code, relèvent du pouvoir réglementaire du Roi.
	Sous-section 2. Certification de cybersécurité obligatoire
	Art. XV.30/4. § 1er. En matière de certification européenne de cybersécurité rendue obligatoire en vertu du droit de l'Union ou du droit national, après avis de l'autorité nationale de certification de cybersécurité, le Roi peut, par arrêté délibéré en Conseil des ministres, confier certaines missions en matière de contrôle relatives au règlement sur la cybersécurité ou relatives à la loi du [date] 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, à certains agents du SPF Economie, à condition que ce dernier dispose de l'expertise requise à ces fins.
	§ 2. Les missions en matière de contrôle visées au paragraphe 1er, y compris la recherche, la constatation, la poursuite et la sanction des infractions, s'effectuent conformément aux dispositions du présent livre.
(…)	(…)
TITRE 3. - L'application pénale du présent Code et de ses arrêtés d'exécution	**TITRE 3. - L'application pénale du présent Code et de ses arrêtés d'exécution**
(…)	(…)
CHAPITRE 2. - Les infractions sanctionnées pénalement	**CHAPITRE 2. - Les infractions sanctionnées pénalement**
(…)	(…)
Section 11/3. - Les peines relatives aux infractions aux règlements de l'Union européenne	**Section 11/3. - Les peines relatives aux infractions aux règlements de l'Union européenne**
Art. XV.125/3. Sont punis d'une sanction de niveau 2 ceux qui commettent une infraction à l'article 14 du règlement (UE) n° 524/2013 du	Art. XV.125/3. Sont punis d'une sanction de niveau 2 ceux qui commettent une infraction à l'article 14 du règlement (UE) n° 524/2013 du

Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 2009/22/CE.	Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 2009/22/CE.
Art.XV.125/4. Sont punis d'une sanction de niveau 2, ceux qui enfreignent les dispositions du règlement (UE) n° 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE.	Art.XV.125/4. Sont punis d'une sanction de niveau 2, ceux qui enfreignent les dispositions du règlement (UE) n° 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE.
	Art. XV.125/5. Dans le cadre de la surveillance visée à l'article [XV.30/4], sont punis d'une sanction de niveau 2:
	1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit « élémentaire » qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;
	2° quiconque ne coopère pas lors d'un contrôle en refusant de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle ou ne coopère pas lors d'un contrôle de toute autre manière.
	Art. XV.125/6. Dans le cadre de la surveillance visée à l'article [XV.30/4], sont punis d'une sanction de niveau 3:
	1° le titulaire d'un certificat de cybersécurité rendu obligatoire en vertu du droit de l'Union ou du droit national attestant du niveau d'assurance dit « substantiel » ou « élevé » qui ne se conforme pas aux obligations émanant du schéma de certification de cybersécurité correspondant;

	2° quiconque communique sciemment des informations inexactes ou incomplètes ou se rend coupable de tout autre acte ou omission frauduleuse dans le cadre de l'exécution du Règlement sur la cybersécurité.
(…)	(…)

COÖRDINATIE VAN DE ARTIKELEN

Basistekst	Tekst aangepast aan het wetsontwerp
Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.	**Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector.**
(…)	(…)
Art. 14. § 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 7 april 2019 tot vaststelling van een kader voor de beveiliging 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, en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten:	Art. 14. § 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 7 april 2019 tot vaststelling van een kader voor de beveiliging 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, 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 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 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;	c) de wet van 26 januari 2018 betreffende de postdiensten;

d) de artikelen 14, § 2, 2°, 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°, 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 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;
h) 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, met betrekking tot de sector digitale infrastructuren;	h) 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, met betrekking tot de sector digitale infrastructuren;
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) k) elk bindend besluit aangenomen door:	k) 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;	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;	iii) de Europese Commissie in de sector van de elektronische communicatie of in de postsector;
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, 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;	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, 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	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.	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 Instituut oefent 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 [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit].
§ 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	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;	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 en aan Berec;	a) de Europese Commissie, ENISA, het Bureau en aan Berec;
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, 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 die belast is met statistiek en economische informatie;	i) de federale overheidsdienst die belast is met statistiek en economische informatie;
j) de ministers bedoeld in artikel 105, § 1, derde lid, 1°, van de wet van 13 juni 2005 betreffende	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.	de elektronische communicatie en hun kabinet, voor de uitvoering van dit artikel.
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;	- waken over de belangen van de gebruikers van postdiensten;
- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;	- bijdragen tot de ontwikkeling van een interne markt voor postdiensten;
- het bevorderen van de concurrentie in de postsector;	- het bevorderen van de concurrentie in de postsector;
7° kan, in de hoedanigheid van inspectiedienst, de mededeling van het beveiligingsplan van de	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.	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.
§ 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.
(…)	(…)
Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten	**Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten**
(…)	(…)
Art. 45. § 1. De FSMA heeft als opdracht, overeenkomstig deze wet en de bijzondere wetten die op haar van toepassing zijn:	Art. 45. § 1. De FSMA heeft als opdracht, overeenkomstig deze wet en de bijzondere wetten die op haar van toepassing zijn:
1° toe te zien op de naleving van de regels die de bescherming van de belangen van de belegger beogen bij verrichtingen in financiële instrumenten en andere beleggingsinstrumenten, en op de naleving van de regels die de goede werking, de integriteit en de transparantie van de markten voor financiële instrumenten en andere beleggingsinstrumenten moeten waarborgen, en meer in het bijzonder van de regels bedoeld in hoofdstuk II, de bepalingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van richtlijn 2014/65/EU en de besluiten en reglementen genomen ter uitvoering van al het voorgaande;	1° toe te zien op de naleving van de regels die de bescherming van de belangen van de belegger beogen bij verrichtingen in financiële instrumenten en andere beleggingsinstrumenten, en op de naleving van de regels die de goede werking, de integriteit en de transparantie van de markten voor financiële instrumenten en andere beleggingsinstrumenten moeten waarborgen, en meer in het bijzonder van de regels bedoeld in hoofdstuk II, de bepalingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van richtlijn 2014/65/EU en de besluiten en reglementen genomen ter uitvoering van al het voorgaande;
2° het toezicht te verzekeren op:	2° het toezicht te verzekeren op:
a. de vennootschappen voor vermogensbeheer en beleggingsadvies bedoeld in de wet van 25 oktober 2016, de beheervennootschappen van instellingen voor collectieve belegging, de	a. de vennootschappen voor vermogensbeheer en beleggingsadvies bedoeld in de wet van 25 oktober 2016, de beheervennootschappen van instellingen voor collectieve belegging, de

beheerders van AICB's bedoeld in de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders, en de wisselkantoren bedoeld in de wet van 25 oktober 2016 en haar uitvoeringsbesluiten;	beheerders van AICB's bedoeld in de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders, en de wisselkantoren bedoeld in de wet van 25 oktober 2016 en haar uitvoeringsbesluiten;
b. de instellingen voor collectieve belegging bedoeld in de wet van 3 augustus 2012 betreffende de instellingen voor collectieve belegging die voldoen aan de voorwaarden van richtlijn 2009/65/EG en de instellingen voor belegging in schuldvorderingen, en in de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders;	b. de instellingen voor collectieve belegging bedoeld in de wet van 3 augustus 2012 betreffende de instellingen voor collectieve belegging die voldoen aan de voorwaarden van richtlijn 2009/65/EG en de instellingen voor belegging in schuldvorderingen, en in de wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders;
c. [...];	c. [...];
d. de ondernemingen en de verrichtingen bedoeld in de wet van 12 juni 1991 op het consumentenkrediet;	d. de ondernemingen en de verrichtingen bedoeld in de wet van 12 juni 1991 op het consumentenkrediet;
[...]	[...]
e. de verzekerings- en herverzekeringstussenpersonen bedoeld in de wet van 4 april 2014 betreffende de verzekeringen;	e. de verzekerings- en herverzekeringstussenpersonen bedoeld in de wet van 4 april 2014 betreffende de verzekeringen;
f. de tussenpersonen in bank- en beleggingsdiensten bedoeld in de wet van 22 maart 2006 betreffende de bemiddeling in bank- en beleggingsdiensten en de distributie van financiële instrumenten;	f. de tussenpersonen in bank- en beleggingsdiensten bedoeld in de wet van 22 maart 2006 betreffende de bemiddeling in bank- en beleggingsdiensten en de distributie van financiële instrumenten;
g. [...]	g. [...]
h. de gereglementeerde vastgoedvennootschappen bedoeld in de wet van 12 mei 2014 betreffende de gereglementeerde vastgoedvennootschappen;	h. de gereglementeerde vastgoedvennootschappen bedoeld in de wet van 12 mei 2014 betreffende de gereglementeerde vastgoedvennootschappen;
i. de onafhankelijk financieel planners als bedoeld in de wet van 25 april 2014 inzake het statuut van en het toezicht op de onafhankelijk financieel planners en inzake het verstrekken van raad over financiële planning door gereglementeerde ondernemingen;	i. de onafhankelijk financieel planners als bedoeld in de wet van 25 april 2014 inzake het statuut van en het toezicht op de onafhankelijk financieel planners en inzake het verstrekken van raad over financiële planning door gereglementeerde ondernemingen;

j. de kredietgevers en de kredietbemiddelaars bedoeld in boek VII, titel 4, hoofdstuk 4, van het Wetboek van economisch recht;	j. de kredietgevers en de kredietbemiddelaars bedoeld in boek VII, titel 4, hoofdstuk 4, van het Wetboek van economisch recht;
k. crowdfundingdienstverleners als bedoeld in Verordening (EU) 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937;	k. crowdfundingdienstverleners als bedoeld in Verordening (EU) 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937;
l. de aanbieders van datarapporteringsdiensten als bedoeld in de wet van 21 november 2017 en houdende omzetting van Richtlijn 2014/65/EU;	l. de aanbieders van datarapporteringsdiensten als bedoeld in de wet van 21 november 2017 en houdende omzetting van Richtlijn 2014/65/EU;
m. de benchmarkbeheerders bedoeld in Verordening (EU) 2016/1011;	m. de benchmarkbeheerders bedoeld in Verordening (EU) 2016/1011;
n. de aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta en de aanbieders van bewaarportemonnees als bedoeld in artikel 5, § 1, eerste lid, 14° /1 en 14° /2, 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, en in het ter uitvoering van artikel 5, § 1, tweede lid, van dezelfde wet genomen besluit.	n. de aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta en de aanbieders van bewaarportemonnees als bedoeld in artikel 5, § 1, eerste lid, 14° /1 en 14° /2, 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, en in het ter uitvoering van artikel 5, § 1, tweede lid, van dezelfde wet genomen besluit.
3° toe te zien op de naleving door de kredietinstellingen, de verzekeringsondernemingen, de herverzekeringsondernemingen, de beursvennootschappen, de centrale tegenpartijen, de transactieregisters, de centrale effectenbewaarinstellingen, de instellingen die ondersteuning verlenen aan centrale effectenbewaarinstellingen, en de depositobanken, van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen, voor zover die op hen van toepassing zijn:	3° toe te zien op de naleving door de kredietinstellingen, de verzekeringsondernemingen, de herverzekeringsondernemingen, de beursvennootschappen, de centrale tegenpartijen, de transactieregisters, de centrale effectenbewaarinstellingen, de instellingen die ondersteuning verlenen aan centrale effectenbewaarinstellingen, en de depositobanken, van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen, voor zover die op hen van toepassing zijn:
a. de regels bedoeld in hoofdstuk II;	a. de regels bedoeld in hoofdstuk II;
b. de wet van 25 juni 1992 op de landverzekeringsovereenkomst;	b. de wet van 25 juni 1992 op de landverzekeringsovereenkomst;
c. de wet van 4 april 2014 betreffende de verzekeringen;	c. de wet van 4 april 2014 betreffende de verzekeringen;

d. de wet van 22 maart 2006 betreffende de bemiddeling in bank- en beleggingsdiensten en de distributie van financiële instrumenten;	d. de wet van 22 maart 2006 betreffende de bemiddeling in bank- en beleggingsdiensten en de distributie van financiële instrumenten;
e. [...];	e. [...];
f. artikel 42 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, de artikelen 21, 41 tot 42/2,, 64, 65 § 3, 65/2 en 65/3, evenals artikel 66 voor wat betreft het verstrekken van beleggingsdiensten en het verrichten van beleggingsactiviteiten, van de wet van 25 april 2014, de artikelen 502, 510, 510/1, 510/2, 527, 528, 529/1 evenals 530 voor wat betreft het verstrekken van beleggingsdiensten en het verrichten van beleggingsactiviteiten, van de diezelfde wet voor zover de artikelen 502 en 528, eerste lid, van die wet de voormelde artikelen 21 en 65, § 3, van toepassing verklaren op de beursvennootschappen, vanuit het oogpunt van de naleving van de regels die een loyale, billijke en professionele behandeling van de belanghebbende partijen moeten waarborgen;	f. artikel 42 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, de artikelen 21, 41 tot 42/2,, 64, 65 § 3, 65/2 en 65/3, evenals artikel 66 voor wat betreft het verstrekken van beleggingsdiensten en het verrichten van beleggingsactiviteiten, van de wet van 25 april 2014, de artikelen 502, 510, 510/1, 510/2, 527, 528, 529/1 evenals 530 voor wat betreft het verstrekken van beleggingsdiensten en het verrichten van beleggingsactiviteiten, van de diezelfde wet voor zover de artikelen 502 en 528, eerste lid, van die wet de voormelde artikelen 21 en 65, § 3, van toepassing verklaren op de beursvennootschappen, vanuit het oogpunt van de naleving van de regels die een loyale, billijke en professionele behandeling van de belanghebbende partijen moeten waarborgen;
g. de artikelen 65, §§ 1 en 2, en 528, eerste lid van de wet van 25 april 2014, voor zover dit laatste artikel het voormelde artikel 65, §§ 1 en 2, van toepassing verklaart op de beursvennootschappen;	g. de artikelen 65, §§ 1 en 2, en 528, eerste lid van de wet van 25 april 2014, voor zover dit laatste artikel het voormelde artikel 65, §§ 1 en 2, van toepassing verklaart op de beursvennootschappen;
h) in de bepalingen bedoeld in artikel 16, § 7, van de wet van 13 november 2011 betreffende de vergoeding van de lichamelijke en morele schade ingevolge een technologisch ongeval;	h) in de bepalingen bedoeld in artikel 16, § 7, van de wet van 13 november 2011 betreffende de vergoeding van de lichamelijke en morele schade ingevolge een technologisch ongeval;
i. de wet van 25 april 2014 inzake het statuut van en het toezicht op de onafhankelijk financieel planners en inzake het verstrekken van raad over financiële planning door gereglementeerde ondernemingen;	i. de wet van 25 april 2014 inzake het statuut van en het toezicht op de onafhankelijk financieel planners en inzake het verstrekken van raad over financiële planning door gereglementeerde ondernemingen;
j. Artikel 383 van de wet van 25 april 2014;	j. Artikel 383 van de wet van 25 april 2014;
k. Titel II van de wet van 18 december 2016 tot regeling van de erkenning en de afbakening van crowdfunding en houdende diverse bepalingen inzake financiën;	k. Titel II van de wet van 18 december 2016 tot regeling van de erkenning en de afbakening van crowdfunding en houdende diverse bepalingen inzake financiën;

4° toe te zien op de naleving van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen:	4° toe te zien op de naleving van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen:
a. Titel II, hoofdstuk 1, afdeling 4 van de programmawet (I) van 24 december 2002 betreffende de aanvullende pensioenen voor zelfstandigen;	a. Titel II, hoofdstuk 1, afdeling 4 van de programmawet (I) van 24 december 2002 betreffende de aanvullende pensioenen voor zelfstandigen;
b. de wet van 28 april 2003 betreffende de aanvullende pensioenen en het belastingstelsel van die pensioenen en van sommige aanvullende voordelen inzake sociale zekerheid;	b. de wet van 28 april 2003 betreffende de aanvullende pensioenen en het belastingstelsel van die pensioenen en van sommige aanvullende voordelen inzake sociale zekerheid;
c. titel 4 van de wet van 15 mei 2014 houdende diverse bepalingen, wat het aanvullend pensioen voor bedrijfsleiders betreft;	c. titel 4 van de wet van 15 mei 2014 houdende diverse bepalingen, wat het aanvullend pensioen voor bedrijfsleiders betreft;
d. titel II van de wet van 18 februari 2018 houdende diverse bepalingen inzake aanvullende pensioenen en tot instelling van een aanvullend pensioen voor de zelfstandigen actief als natuurlijk persoon, voor de meewerkende echtgenoten en voor de zelfstandige helpers;	d. titel II van de wet van 18 februari 2018 houdende diverse bepalingen inzake aanvullende pensioenen en tot instelling van een aanvullend pensioen voor de zelfstandigen actief als natuurlijk persoon, voor de meewerkende echtgenoten en voor de zelfstandige helpers;
e. titel 2 van de wet van 6 december 2018 tot instelling van een vrij aanvullend pensioen voor de werknemers en houdende diverse bepalingen inzake aanvullende pensioenen;	e. titel 2 van de wet van 6 december 2018 tot instelling van een vrij aanvullend pensioen voor de werknemers en houdende diverse bepalingen inzake aanvullende pensioenen;
e. artikel 12 van de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie, in de mate dat artikel 32 van die wet voorziet in de bevoegdheid van de FSMA, en artikel 12 van de wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen, in de mate dat artikel 38 van die wet voorziet in de bevoegdheid van de FSMA;	e. artikel 12 van de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie, in de mate dat artikel 32 van die wet voorziet in de bevoegdheid van de FSMA, en artikel 12 van de wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen, in de mate dat artikel 38 van die wet voorziet in de bevoegdheid van de FSMA;
4° /1 toe te zien op de naleving van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen:	4° /1 toe te zien op de naleving van de volgende bepalingen en de ter uitvoering ervan genomen besluiten en reglementen:
a. de bepalingen bedoeld in artikel 15, eerste lid, van de wet van 21 december 2013 betreffende diverse bepalingen inzake de financiering voor kleine en middelgrote ondernemingen;	a. de bepalingen bedoeld in artikel 15, eerste lid, van de wet van 21 december 2013 betreffende diverse bepalingen inzake de financiering voor kleine en middelgrote ondernemingen;
b. de bepalingen bedoeld in artikel 17, § 1, van de wet van 26 december 2013 houdende diverse	b. de bepalingen bedoeld in artikel 17, § 1, van de wet van 26 december 2013 houdende diverse

bepalingen inzake de thematische volksleningen;	bepalingen inzake de thematische volksleningen;
5° bij te dragen tot de naleving van de regels bedoeld om de afnemers van financiële producten of diensten en kredietnemers te beschermen tegen het onwettelijk aanbod of de illegale levering van financiële producten of diensten of van kredieten en tegen het onrechtmatige gebruik van benamingen die zijn voorbehouden aan ondernemingen die door de FSMA of de Bank zijn vergund, ingeschreven of geregistreerd;	5° bij te dragen tot de naleving van de regels bedoeld om de afnemers van financiële producten of diensten en kredietnemers te beschermen tegen het onwettelijk aanbod of de illegale levering van financiële producten of diensten of van kredieten en tegen het onrechtmatige gebruik van benamingen die zijn voorbehouden aan ondernemingen die door de FSMA of de Bank zijn vergund, ingeschreven of geregistreerd;
6° bij te dragen tot de financiële vorming;	6° bij te dragen tot de financiële vorming;
7° bij te dragen tot de naleving van de bepalingen van boek VI van het Wetboek economisch recht en de ter uitvoering ervan genomen besluiten en reglementen die betrekking hebben op financiële diensten als bedoeld in boek I van hetzelfde Wetboek door de ondernemingen die onder haar toezicht staan of waarvan de verrichtingen of producten onder haar toezicht staan.	7° bij te dragen tot de naleving van de bepalingen van boek VI van het Wetboek economisch recht en de ter uitvoering ervan genomen besluiten en reglementen die betrekking hebben op financiële diensten als bedoeld in boek I van hetzelfde Wetboek door de ondernemingen die onder haar toezicht staan of waarvan de verrichtingen of producten onder haar toezicht staan.
Op advies van de Bank en de FSMA, en om met name rekening te houden met de stand van de Europese reglementering ter zake, kan de Koning voor de uitvoering van de bepalingen bedoeld in het eerste lid, 3°, en voor het toezicht door de FSMA op de naleving van die bepalingen door de instellingen of personen bedoeld in het eerste lid, 2° of 3°, een onderscheid maken tussen professionele en niet-professionele belanghebbende partijen of tussen sommige categorieën van professionele belanghebbende partijen onderling.	Op advies van de Bank en de FSMA, en om met name rekening te houden met de stand van de Europese reglementering ter zake, kan de Koning voor de uitvoering van de bepalingen bedoeld in het eerste lid, 3°, en voor het toezicht door de FSMA op de naleving van die bepalingen door de instellingen of personen bedoeld in het eerste lid, 2° of 3°, een onderscheid maken tussen professionele en niet-professionele belanghebbende partijen of tussen sommige categorieën van professionele belanghebbende partijen onderling.
In afwijking van het eerste lid, behoort het toezicht op de naleving van de regels bedoeld in het eerste lid, 3°, en § 2, door de maatschappijen van onderlinge bijstand bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen tot de bevoegdheid van de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen.	In afwijking van het eerste lid, behoort het toezicht op de naleving van de regels bedoeld in het eerste lid, 3°, en § 2, door de maatschappijen van onderlinge bijstand bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen tot de bevoegdheid van de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen.

De FSMA heeft eveneens als opdracht, in de mate waarin 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 hierin voorziet, toe te zien op de naleving door de onderworpen entiteiten bedoeld in artikel 85, § 1, 4°, van dezelfde wet, van de wettelijke en reglementaire of Europeesrechtelijke bepalingen die strekken tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, evenals van de financiering van de proliferatie van massavernietigingswapens.	De FSMA heeft eveneens als opdracht, in de mate waarin 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 hierin voorziet, toe te zien op de naleving door de onderworpen entiteiten bedoeld in artikel 85, § 1, 4°, van dezelfde wet, van de wettelijke en reglementaire of Europeesrechtelijke bepalingen die strekken tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, evenals van de financiering van de proliferatie van massavernietigingswapens.
§ 2. Teneinde de loyale, billijke en professionele behandeling van de belanghebbende partijen te bevorderen kan de Koning, op advies van de FSMA en de Bank, voor de instellingen en personen bedoeld in § 1, eerste lid, 2° en 3°, de regels bedoeld in § 1, eerste lid, 3°, uitbreiden met bepalingen die betrekking hebben op:	§ 2. Teneinde de loyale, billijke en professionele behandeling van de belanghebbende partijen te bevorderen kan de Koning, op advies van de FSMA en de Bank, voor de instellingen en personen bedoeld in § 1, eerste lid, 2° en 3°, de regels bedoeld in § 1, eerste lid, 3°, uitbreiden met bepalingen die betrekking hebben op:
- de informatieverplichtingen aan de belanghebbende partijen;	- de informatieverplichtingen aan de belanghebbende partijen;
- de contractuele verplichtingen en voorwaarden;	- de contractuele verplichtingen en voorwaarden;
- de verplichting de belangen van de cliënten optimaal te verzorgen (zorgplicht);	- de verplichting de belangen van de cliënten optimaal te verzorgen (zorgplicht);
- regelingen inzake de voordelen die verband houden met de verstrekte diensten;	- regelingen inzake de voordelen die verband houden met de verstrekte diensten;
- het verstrekken van diensten via internet;	- het verstrekken van diensten via internet;
- de publiciteitsregels;	- de publiciteitsregels;
- de klachtenbehandeling;	- de klachtenbehandeling;
- transparantie, via de verplichte vermelding van een label of anderszins, over risico's, prijzen, vergoedingen en kosten;	- transparantie, via de verplichte vermelding van een label of anderszins, over risico's, prijzen, vergoedingen en kosten;
- toegankelijkheid van de verstrekte diensten.	- toegankelijkheid van de verstrekte diensten.
Hij kan inzonderheid verschillende regels bepalen naargelang het gaat om professionele of niet-professionele belanghebbende partijen of	Hij kan inzonderheid verschillende regels bepalen naargelang het gaat om professionele of niet-professionele belanghebbende partijen of

tussen sommige categorieën van professionele belanghebbende partijen onderling.	tussen sommige categorieën van professionele belanghebbende partijen onderling.
§ 3. Voor de toepassing van dit artikel worden met " belanghebbende partijen " bedoeld, de cliënten en potentiële cliënten van de betrokken ondernemingen, de verzekeringsnemers, de verzekerden en de begunstigden van de bij de verzekeringsondernemingen afgesloten verzekeringsovereenkomsten.	§ 3. Voor de toepassing van dit artikel worden met " belanghebbende partijen " bedoeld, de cliënten en potentiële cliënten van de betrokken ondernemingen, de verzekeringsnemers, de verzekerden en de begunstigden van de bij de verzekeringsondernemingen afgesloten verzekeringsovereenkomsten.
§ 4. De bepalingen van de artikelen 36 en 37 zijn van toepassing ingeval de in § 1, eerste lid, 3°, f en g, vermelde regels of de krachtens § 2 opgelegde verplichtingen niet worden nageleefd.	§ 4. De bepalingen van de artikelen 36 en 37 zijn van toepassing ingeval de in § 1, eerste lid, 3°, f en g, vermelde regels of de krachtens § 2 opgelegde verplichtingen niet worden nageleefd.
§ 5. Bij de uitoefening van haar taken houdt de FSMA in de hoedanigheid van bevoegde prudentiële autoriteit rekening met de convergentie van de toezichtinstrumenten en -praktijken bij de toepassing van de wettelijke en bestuursrechtelijke bepalingen die overeenkomstig de toepasselijke Europese richtlijnen zijn vastgesteld.	§ 5. Bij de uitoefening van haar taken houdt de FSMA in de hoedanigheid van bevoegde prudentiële autoriteit rekening met de convergentie van de toezichtinstrumenten en -praktijken bij de toepassing van de wettelijke en bestuursrechtelijke bepalingen die overeenkomstig de toepasselijke Europese richtlijnen zijn vastgesteld.
Daartoe dient zij:	Daartoe dient zij:
a) deel te nemen aan de werkzaamheden van de Europese Bankautoriteit;	a) deel te nemen aan de werkzaamheden van de Europese Bankautoriteit;
b) zich te houden aan de richtsnoeren, aanbevelingen, normen en andere door de Europese Bankautoriteit vastgestelde maatregelen en als zij dat niet doet daarvoor de redenen aan te voeren.	b) zich te houden aan de richtsnoeren, aanbevelingen, normen en andere door de Europese Bankautoriteit vastgestelde maatregelen en als zij dat niet doet daarvoor de redenen aan te voeren.
De FSMA neemt in haar hoedanigheid van bevoegde prudentiële autoriteit bij de uitoefening van haar algemene taken naar behoren de mogelijke gevolgen in overweging die haar besluiten, met name in noodsituaties, kunnen hebben voor de stabiliteit van het financiële stelsel van alle andere betrokken lidstaten, uitgaande van de op het desbetreffende tijdstip beschikbare informatie.	De FSMA neemt in haar hoedanigheid van bevoegde prudentiële autoriteit bij de uitoefening van haar algemene taken naar behoren de mogelijke gevolgen in overweging die haar besluiten, met name in noodsituaties, kunnen hebben voor de stabiliteit van het financiële stelsel van alle andere betrokken lidstaten, uitgaande van de op het desbetreffende tijdstip beschikbare informatie.
	§ 6. Op verzoek van de FSMA en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde

	over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit] volledig of gedeeltelijk aan de FSMA toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de FSMA. De FSMA vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens paragraaf 1, 2°, van dit artikel en de bijzondere wetten die het toezicht op de financiële instellingen regelen.
(…)	(…)
Art. 75. § 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen:	Art. 75. § 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen:
1° aan de Europese Centrale Bank, aan de 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.	1° aan de Europese Centrale Bank, aan de 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.
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 beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van	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 beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van

de wet van 25 oktober 2016, kan de FSMA 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 samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel.	de wet van 25 oktober 2016, kan de FSMA 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 samenhangende 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 FSMA 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 FSMA 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;
1° *bis* aan de Bank , aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB;	1° *bis* aan de Bank , aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB;
2° aan het Federaal Agentschap van de Schuld;	2° aan het Federaal Agentschap van de Schuld;
3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45;	3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45;
4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;	4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;
5° , aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor	5° , aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor

Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening;	Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening;
6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren;	6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren;
7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;	7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;
8° , aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten;	8° , aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten;
9° 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 ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld;	9° 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 ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld;
10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen;	10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen;
11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd;	11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd;

12° 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 ondernemingen die onder het toezicht van de FSMA staan;	12° 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 ondernemingen die onder het toezicht van de FSMA staan;
13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;	13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten;
14° aan de Belgische Mededingingsautoriteit;	14° aan de Belgische Mededingingsautoriteit;
15° aan de autoriteiten bedoeld in artikel 7 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 voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	15° aan de autoriteiten bedoeld in artikel 7 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 voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;
16° aan de Algemene Administratie van de Thesaurie als een dergelijke mededeling is voorgeschreven door het recht van de Europese Unie of door een wettelijke of reglementaire bepaling over financiële sancties (met name de bindende bepalingen betreffende financiële embargo's als gedefinieerd in artikel 4, 6° 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) of als de Algemene Administratie van de Thesaurie optreedt in de hoedanigheid van toezichthouder die zorgt voor 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	16° aan de Algemene Administratie van de Thesaurie als een dergelijke mededeling is voorgeschreven door het recht van de Europese Unie of door een wettelijke of reglementaire bepaling over financiële sancties (met name de bindende bepalingen betreffende financiële embargo's als gedefinieerd in artikel 4, 6° 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) of als de Algemene Administratie van de Thesaurie optreedt in de hoedanigheid van toezichthouder die zorgt voor 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;	en daarop gebaseerde of daaruit voortvloeiende handelingen;
17° , aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;	17° , aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast;
18° aan Fedris;	18° aan Fedris;
19° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen in zijn hoedanigheid van toezichthouder op de maatschappijen voor onderlinge bijstand zoals bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen alsook op hun verrichtingen.	19° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen in zijn hoedanigheid van toezichthouder op de maatschappijen voor onderlinge bijstand zoals bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen alsook op hun verrichtingen.
20° [...]	20° [...]
21° , aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's.	21° , aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's.
22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten;	22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten;
23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten.	23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten.
24° aan de Belgische Gegevensbeschermingsautoriteit.	24° aan de Belgische Gegevensbeschermingsautoriteit.
24° aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 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;	24° aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 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;
25° tijdens procedures tot vereffening van een instelling voor bedrijfspensioenvoorziening of van een pensioenregeling in de zin van de wet	25° tijdens procedures tot vereffening van een instelling voor bedrijfspensioenvoorziening of van een pensioenregeling in de zin van de wet

van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening, aan de autoriteiten en personen die betrokken zijn bij die procedures, alsook aan de autoriteiten die verantwoordelijk zijn voor het toezicht op die autoriteiten en personen;	van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening, aan de autoriteiten en personen die betrokken zijn bij die procedures, alsook aan de autoriteiten die verantwoordelijk zijn voor het toezicht op die autoriteiten en personen;
26° aan de personen die bij de FSMA een klacht hebben ingediend met toepassing van artikel 38 van Verordening 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937, alsook aan de crowdfundingdienstverleners, voor zover nodig voor de behandeling van die klacht.	26° aan de personen die bij de FSMA een klacht hebben ingediend met toepassing van artikel 38 van Verordening 2020/1503 van het Europees Parlement en de Raad van 7 oktober 2020 betreffende Europese crowdfundingdienstverleners voor bedrijven en tot wijziging van Verordening (EU) 2017/1129 en Richtlijn (EU) 2019/1937, alsook aan de crowdfundingdienstverleners, voor zover nodig voor de behandeling van die klacht.
	27° aan de autoriteit bedoeld in artikel 5, § 1, van de wet van […] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit of aan de door de Koning aangewezen overheden krachtens artikel 5, § 2, van dezelfde wet.
(…)	(…)
Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België	**Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België**
(…)	(…)
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:	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° 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	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.	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 en beursvennootschappen, 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 samenhangende 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 en beursvennootschappen, 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 samenhangende 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 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° 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;
2° /1 binnen de grenzen van het recht van de Europese Unie, aan de bevoegde autoriteiten	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;	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 vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt;	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;
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 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	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;	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 bedrijfspensioenen en aan de Europese Bankautoriteit;	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;
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	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 autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 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;	dreiging, aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 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° /1 binnen de grenzen van het recht van de Europese Unie, aan de politiediensten en aan de autoriteit bedoeld in artikel 7, § 1, 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 - NIS-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 autoriteit bedoeld in artikel 7, § 1, 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 - NIS-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 […] 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 onderlinge bijstand als bedoeld in artikel 43bis, § 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;	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 43bis, § 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 12ter, § 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 12ter, § 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;
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 en beursvennootschappen;	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 en beursvennootschappen;
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 beursvennootschappen; en	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 beursvennootschappen; en
c) de speciaal commissaris bedoeld in artikel 236, § 1, 1°, van de voornoemde wet, in artikel 517, § 1, 1°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, artikel 35, § 1, tweede lid, 1°, van de wet van 21 december 2009 op het statuut van de betalingsinstellingen en van 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 87, § 1, tweede lid, 1°, van de voornoemde wet, artikel 48, eerste lid, 1°, van het koninklijk besluit van 30 april 1999	c) de speciaal commissaris bedoeld in artikel 236, § 1, 1°, van de voornoemde wet, in artikel 517, § 1, 1°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, artikel 35, § 1, tweede lid, 1°, van de wet van 21 december 2009 op het statuut van de betalingsinstellingen en van 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 87, § 1, tweede lid, 1°, van de voornoemde wet, artikel 48, eerste lid, 1°, van het koninklijk besluit van 30 april 1999

betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling en artikel 36/30, § 1, tweede lid, 3°, van deze wet;	betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling en artikel 36/30, § 1, tweede lid, 3°, van deze wet;
24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019 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 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019 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.
(…)	(…)
HOOFDSTUK IV/4. - Specifieke opdrachten van de Bank in verband met het voorkomen en het beheer van crisissen en risico's in de financiële sector.	**HOOFDSTUK IV/4. - Specifieke opdrachten van de Bank in verband met het voorkomen en het beheer van crisissen en risico's in de financiële sector.**
(…)	(…)
Art. 36/48. De Bank oefent de opdrachten uit waarmee zij als sectorale overheid voor de sector financiën is belast krachtens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.	Art. 36/48. De Bank oefent de opdrachten uit waarmee zij als sectorale overheid voor de sector financiën is belast krachtens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.
	Art. 36/48/1. Op verzoek van de Bank en naargelang het voorwerp van de betrokken cyberbeveiligingscertificeringsregeling kan de Koning, op voorwaarde dat eerstgenoemde over de daarvoor vereiste expertise beschikt, bij besluit vastgesteld na overleg in de Ministerraad, de opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de

	certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], volledig of gedeeltelijk aan de Bank toevertrouwen. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet en de Bank. De Bank vervult die toezichtsopdrachten enkel ten aanzien van entiteiten waarop zij toezicht uitoefent krachtens de artikelen 8 en 12bis en de bijzondere wetten die het toezicht op de financiële instellingen regelen.
Art. 36/49. De Bank wordt aangeduid als administratieve overheid in de zin van artikel 22*quinquies* 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.	Art. 36/49. De Bank wordt aangeduid als administratieve overheid in de zin van artikel 22*quinquies* 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.
(…)	(…)
Wetboek van economisch recht	**Wetboek van economisch recht**
(…)	(…)
Art. I.20. Voor de toepassing van boek XV gelden de volgende definities:	Art. I.20. Voor de toepassing van boek XV gelden de volgende definities:
1° persoonsgegevens: informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in overeenstemming met de definitie van artikel 1, § 1, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;	1° persoonsgegevens: informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in overeenstemming met de definitie van artikel 1, § 1, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;
2° verantwoordelijke voor de verwerking: de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt;	2° verantwoordelijke voor de verwerking: de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt;
3° verwerking: elke bewerking of elk geheel van bewerkingen met betrekking tot	3° verwerking: elke bewerking of elk geheel van bewerkingen met betrekking tot

persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens;	persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens;
4° federale coördinator: de natuurlijke persoon benoemd binnen de Federale Overheidsdienst Economie, om in het kader van de administratieve samenwerking, bepaald in de artikelen XV.35 tot XV.48, het aanspreekpunt te zijn tussen de Europese Commissie en de bevoegde Belgische autoriteiten;	4° federale coördinator: de natuurlijke persoon benoemd binnen de Federale Overheidsdienst Economie, om in het kader van de administratieve samenwerking, bepaald in de artikelen XV.35 tot XV.48, het aanspreekpunt te zijn tussen de Europese Commissie en de bevoegde Belgische autoriteiten;
5° waarschuwingscoördinator: de natuurlijke persoon of personen die op federaal niveau is of zijn aangewezen om de andere lidstaten en de Europese Commissie in kennis te stellen van ernstige specifieke handelingen of omstandigheden met betrekking tot een dienstenactiviteit, die ernstige schade aan de gezondheid of veiligheid van personen of aan het milieu kunnen veroorzaken;	5° waarschuwingscoördinator: de natuurlijke persoon of personen die op federaal niveau is of zijn aangewezen om de andere lidstaten en de Europese Commissie in kennis te stellen van ernstige specifieke handelingen of omstandigheden met betrekking tot een dienstenactiviteit, die ernstige schade aan de gezondheid of veiligheid van personen of aan het milieu kunnen veroorzaken;
6° Bank: de Nationale Bank van België;	6° Bank: de Nationale Bank van België;
7° onderneming: iedere natuurlijke persoon of rechtspersoon die op duurzame wijze een economisch doel nastreeft, alsmede zijn verenigingen;	7° onderneming: iedere natuurlijke persoon of rechtspersoon die op duurzame wijze een economisch doel nastreeft, alsmede zijn verenigingen;
8° nschrijvingsplichtige onderneming: elke entiteit die zich dient in te schrijven krachtens artikel III.49;	8° nschrijvingsplichtige onderneming: elke entiteit die zich dient in te schrijven krachtens artikel III.49;
9° klager in de landbouw- en voedselvoorzieningsketen: elke leverancier van landbouw- en voedingsproducten, elke producentenorganisatie, elke organisatie van leveranciers, elke organisatie waar een producent of leverancier lid van is, elke vereniging van organisaties waar een leverancier lid van is en elke andere organisatie die een rechtmatig belang heeft bij de vertegenwoordiging van leveranciers voor zover het een onafhankelijke rechtspersoon zonder	9° klager in de landbouw- en voedselvoorzieningsketen: elke leverancier van landbouw- en voedingsproducten, elke producentenorganisatie, elke organisatie van leveranciers, elke organisatie waar een producent of leverancier lid van is, elke vereniging van organisaties waar een leverancier lid van is en elke andere organisatie die een rechtmatig belang heeft bij de vertegenwoordiging van leveranciers voor zover het een onafhankelijke rechtspersoon zonder

winstoogmerk betreft, die geconfronteerd wordt met een afnemer van landbouw- en voedingsproducten van wie wordt vermoed dat hij zich schuldig maakt aan een inbreuk op de in artikel XV.83, 15° /1, bedoelde bepalingen.	winstoogmerk betreft, die geconfronteerd wordt met een afnemer van landbouw- en voedingsproducten van wie wordt vermoed dat hij zich schuldig maakt aan een inbreuk op de in artikel XV.83, 15° /1, bedoelde bepalingen.
	10° Cyberbeveiligingsverordening: 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.
(…)	(…)
Boek XV. - Rechtshandhaving	**Boek XV. - Rechtshandhaving**
TITEL 1. - De uitoefening van toezicht en de opsporing en vaststelling van inbreuken	**TITEL 1. - De uitoefening van toezicht en de opsporing en vaststelling van inbreuken**
(…)	(…)
HOOFDSTUK 2. - Bijzondere bevoegdheden	**HOOFDSTUK 2. - Bijzondere bevoegdheden**
(…)	(…)
Afdeling 9. Andere bijzondere bevoegdheden	**Afdeling 9. Andere bijzondere bevoegdheden**
Art. XV.30/2. De door de minister aangestelde ambtenaren zijn bevoegd de controleurs van de Europese Commissie de nodige bijstand te verlenen, zoals bedoeld in artikel 9 van de Verordening (Euratom, EG) nr. 2185/96 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Europese Gemeenschappen tegen fraude en andere onregelmatigheden.	Art. XV.30/2. De door de minister aangestelde ambtenaren zijn bevoegd de controleurs van de Europese Commissie de nodige bijstand te verlenen, zoals bedoeld in artikel 9 van de Verordening (Euratom, EG) nr. 2185/96 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Europese Gemeenschappen tegen fraude en andere onregelmatigheden.
De in het eerste lid bedoelde ambtenaren beschikken daarbij over de bevoegdheden voorzien in titel 1, hoofdstuk 1.	De in het eerste lid bedoelde ambtenaren beschikken daarbij over de bevoegdheden voorzien in titel 1, hoofdstuk 1.
	Afdeling 10. Certificering van de cyberbeveiliging

	Onderafdeling 1. Vrijwillige cyberbeveiligingscertificering
	Art. XV.30/3. Op het gebied van vrijwillige cyberbeveiligingscertificering kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde opdrachten bedoeld in hoofdstuk 5 en 6, met uitzondering van artikel 21 en 22, van de wet van [datum] [inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit], aan bepaalde ambtenaren van de FOD Economie toevertrouwen, op voorwaarde dat de FOD Economie over de daarvoor vereiste expertise beschikt. In dat geval vraagt de Koning het advies van en overlegt Hij vooraf met de autoriteit bedoeld in artikel 5, § 1, van voornoemde wet. De FOD Economie vervult die toezichtsopdrachten enkel ten aanzien van producten of entiteiten die gereglementeerd zijn door dit Wetboek, de uitvoeringsbesluiten ervan of verordeningen van de Europese Unie betreffende aangelegenheden die, overeenkomstig de boeken VI, VII, IX en XII van dit Wetboek, tot de regelgevende bevoegdheid van de Koning behoren.
	Onderafdeling 2. Verplichte cyberbeveiligingscertificering
	Art. XV.30/4. § 1. Met betrekking tot de Europese cyberbeveiligingscertificering die verplicht is op grond van de Europese of nationale wetgeving, na advies van de nationale cyberbeveiligingscertificeringsautoriteit, kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad, bepaalde toezichtsopdrachten in verband met de Cyberbeveiligingsverordening of in verband met de wet van [datum] inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, toevertrouwen aan bepaalde ambtenaren van de FOD Economie, op voorwaarde dat die

	laatste over de voor deze doeleinden vereiste expertise beschikt.
	§ 2. De in de eerste paragraaf bedoelde toezichtsopdrachten, met inbegrip van de opsporing, vaststelling, vervolging en bestraffing van inbreuken, worden uitgeoefend overeenkomstig de bepalingen van dit boek.
(…)	(…)
TITEL 3. - De strafrechtelijke handhaving van dit Wetboek en zijn uitvoeringsbesluiten	**TITEL 3. - De strafrechtelijke handhaving van dit Wetboek en zijn uitvoeringsbesluiten**
(…)	(…)
HOOFDSTUK 2. - De strafrechtelijk gesanctioneerde inbreuken	**HOOFDSTUK 2. - De strafrechtelijk gesanctioneerde inbreuken**
(…)	(…)
Afdeling 11/3. - De straffen voor inbreuken op verordeningen van de Europese Unie	**Afdeling 11/3. - De straffen voor inbreuken op verordeningen van de Europese Unie**
Art. XV.125/3. Met een sanctie van niveau 2 worden bestraft zij die artikel 14 van Verordening (EU) Nr. 524/2013 van het Europees Parlement en de Raad van 21 mei 2013 betreffende onlinebeslechting van consumentengeschillen en tot wijziging van Verordening (EG) nr. 2006/2004 en richtlijn 2009/22/EG overtreden.	Art. XV.125/3. Met een sanctie van niveau 2 worden bestraft zij die artikel 14 van Verordening (EU) Nr. 524/2013 van het Europees Parlement en de Raad van 21 mei 2013 betreffende onlinebeslechting van consumentengeschillen en tot wijziging van Verordening (EG) nr. 2006/2004 en richtlijn 2009/22/EG overtreden.
Art.XV.125/4. Met een sanctie van niveau 2 worden bestraft zij die de bepalingen van verordening (EU) nr. 2018/302 van het Europees Parlement en de Raad van 28 februari 2018 inzake de aanpak van ongerechtvaardigde geoblocking en andere vormen van discriminatie van klanten op grond van nationaliteit, verblijfplaats of plaats van vestiging in de interne markt, en tot wijziging van Verordeningen (EG) nr. 2006/2004 en (EU) 2017/2394 en Richtlijn 2009/22/EG overtreden.	Art.XV.125/4. Met een sanctie van niveau 2 worden bestraft zij die de bepalingen van verordening (EU) nr. 2018/302 van het Europees Parlement en de Raad van 28 februari 2018 inzake de aanpak van ongerechtvaardigde geoblocking en andere vormen van discriminatie van klanten op grond van nationaliteit, verblijfplaats of plaats van vestiging in de interne markt, en tot wijziging van Verordeningen (EG) nr. 2006/2004 en (EU) 2017/2394 en Richtlijn 2009/22/EG overtreden.
	Art. XV.125/5. Wordt in het kader van het toezicht bedoeld in artikel [XV.30/4] gestraft met een sanctie van niveau 2:

	1° de houder van een cyberbeveiligingscertificaat dat verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "basis" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken Europese cyberbeveiligingscertificeringsregeling;
	2° eenieder die niet meewerkt tijdens een inspectie door te weigeren de naar aanleiding van deze inspectie gevraagde informatie te verstrekken of die anderszins weigert mee te werken tijdens een inspectie.
	Art. XV.125/6. Wordt in het kader van het toezicht bedoeld in artikel [XV.30/4] gestraft met een sanctie van niveau 3:
	1° de houder van een cyberbeveiligingscertificaat dat verplicht is op grond van de Europese of nationale wetgeving voor zekerheidsniveau "substantieel" of "hoog" die niet voldoet aan de verplichtingen die voortvloeien uit de betrokken cyberbeveiligingscertificeringsregeling;
	2° eenieder die bewust onjuiste of onvolledige informatie verstrekt of zich schuldig maakt aan enige andere frauduleuze handeling of nalatigheid in het kader van de uitvoering van de Cyberbeveiligingsverordening.
(…)	(…)

ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
/	DA210031		19.01.2022

Objet : **Avis relatif à l'avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité**

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou '!'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED).*

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

Vu la demande adressée par le premier ministre en date du 30 novembre 2021.

Attendu que l'Autorité de protection des données a transmis la demande à l'Organe de contrôle en date du 7 décembre 2021.

Vu le rapport de Monsieur Koen Gorissen, membre-conseiller de l'Organe de contrôle.

Émet, le 19 janvier 2022, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la LAPD dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice ou *LED)*. L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après

---

[1] 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 « RGPD »).

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAJ. du Conseil (ci-après dénommée « directive Police-Justice» ou *Law Enforcement Directive (LEO))*.

[3] Article 4 §2, 4• alinéa de la LAPD.

[4] Article 71 §1•', 3• alinéa de la LPD.

[5] Articles 59 §1er, 2• alinéa et 236 §2 de la LPD.

dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. Enfin, l'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale sur les douanes et accises du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

II. Objet de la demande

S. Le premier ministre a adressé en date du 30 novembre 2021 à l'Autorité de protection des données une demande d'avis concernant un avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (ci-après *'l'avant-projet?*.

6. En application de l'article 54/1 de la LAPD, l'Autorité de protection des données a transmis la demande en date du 7 décembre 2021 à l'Organe de contrôle de l'information policière afin que ce dernier émette un avis sur l'avant-projet.

7. L'Organe de contrôle souligne que les autorités et les traitements de données à caractère personnel et d'informations qui relèvent exclusivement de sa compétence sont strictement définis par la loi et qu'il limite par conséquent ses avis aux traitements relevant de sa compétence, à savoir les traitements effectués par les services de police.

8. Toutefois, les avis du COC ne se limitent pas nécessairement à l'article ou aux articles mentionnés dans la demande d'avis. Le COC tient en effet toujours compte de tous les éléments et dispositions qui relèvent de sa compétence en vertu de la réglementation susmentionnée.

En l'occurrence, cela signifie que les articles 6, 15, 36 et 38 de l'avant-projet sont analysés dans le présent avis.

III. Analyse de la demande

1. À titre principal

[6] Article 71 §1•', troisième alinéa juncto article 236 §3 de la LPD.

9. L'avant-projet met en œuvre le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à la certification de cybersécurité des technologies de l'information et des communication (le règlement sur la cybersécurité) et définit les compétences des services d'inspection, les sanctions, les procédures de plainte et de recours, les autorisations légales requises pour certaines délégations, les règles générales en matière d'indépendance, etc. L'avant-projet permet aussi l'échange d'informations entre l'autorité de certification de cybersécurité et les autres autorités. Si les informations sont des données à caractère personnel, les modalités de cet échange sont fixées au chapitre 8 de l'avant-projet7.

10. L'autorité de certification de cybersécurité peut échanger des données à caractère personnel avec d'autres autorités[8] (dont aussi des services de police) si cet échange est nécessaire au respect des obligations légales découlant du règlement sur la cybersécurité ou de l'avant-projet, ou encore à l'accomplissement d'une mission d'intérêt général qui a été confiée à l'une des autorités publiques visées par l'avant-projet.

Les données à caractère personnel pouvant être échangées sur la base de l'avant-projet sont plus particulièrement des données d'identification ou d'authentification et des données de communications électroniques des catégories suivantes de personnes :

toute personne intervenant pour :
- des organismes d'évaluation de la conformité,
- des titulaires de certificats de cybersécurité européens,
- des émetteurs de déclarations de conformité de l'Union européenne,
- une autorité publique ;

toute personne participant à un contrôle ou à une audition dans le cadre des missions de contrôle de l'autorité de certification de cybersécurité ;
toute personne qui introduit une réclamation.

L'avant-projet prévoit donc des transferts de données entre l'autorité nationale de certification de cybersécurité (à savoir l'autorité fédérale) et les services de police.

11. Certaines conditions légales doivent être respectées lors des transmissions d'informations avec les services de police. Pour en examiner la conformité, il y a lieu avant tout de déterminer si les transmissions de données dans le cadre de l'avant-projet sont unilatérales ou réciproques.

Conformément à l'avant-projet, des informations policières seront transmises des services de police vers une autorité fédérale étant donné que l'échange d'informations sera possible (voir point 10).

---

[7] Article 6 §3 de l'avant-projet.

[8] Les autorités énumérées à l'artide 36 §1°' de l'avant-projet.

Cette transmission de données doit avoir une base légale et être nécessaire et proportionnée[9]. Pour les services de police, cette base légale est prévue à l'article 44/11/9 de la loi sur la fonction de police (LFP'). Il peut aussi s'agir de l'autorisation du ministère public sur la base de ses prérogatives[10].

12. L'article 44/11/9 de la LFP réglemente la communication de données à caractère personnel et d'informations par les services de police. Son paragraphe 2 prévoit : *« Selon les modalités déterminées par les directives des ministres de /1ntérieur et de la Justice, chacun dans le cadre de ses compétences, elles1[11] peuvent également être communiquées aux autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique lorsque ceux-ci en ont besoin pour /'exécution de leurs missions légales. ».*

L'article 44/11/9 §2 de la LFP fait référence à une liste qui doit énumérer toutes les autorités, tous les organes et tous les organismes auxquels les services de police peuvent communiquer des données à caractère personnel et des informations. Conformément à l'article 44/11/9, cette liste doit être arrêtée par les ministres de 11ntérieur et de la Justice sur la base d'une proposition du Comité information et ICT qui aura recueilli au préalable l'avis de l'Organe de contrôle. Au moment de la rédaction du présent avis, l'Organe de contrôle n'a pas reçu de proposition/demande d'avis de la part du comité susmentionné, et cette liste n'existe pas.

De plus, les dispositions de la LFP exigent un protocole d'accord en cas de communication récurrente ou volumineuse de données à caractère personnel ou informations[12].

En conséquence, ce transfert et son contenu, tels que visés par l'avant-projet, ne sont pas conformes aux dispositions de l'article 44/11/9 de la LFP[13].

13. En ce qui concerne la communication aux services de police d'informations provenant de l'autorité nationale de certification de cybersécurité, l'auteur de l'avant-projet indique que l'échange des données à caractère personnel peut être « mutuel »[14]. Autrement dit, les échanges d'informations entre l'autorité fédérale et les services de police sont bidirectionnels.

Conformément à l'article 44/11/9 §4 de la LFP, les modalités de cette communication doivent être précisées dans un protocole d'accord approuvé.

---

[9] Article 29 §1er de la LPD.
[10] Article 21bis du Code d1nstruction criminelle et article 1380 du Code judiciaire.
[11] Les données à caractère personnel et les informations.
[12] Article 44/11/9 §§2-3 de la LFP.
[13] Voir aussi l'avis du COC relatif à l'avant-projet de décret modifiant le décret du 6 mai 2019 relatif à la délinquance environnementale et divers autres décrets (DA210008), 21 mai 2021, httDs://www.organedecontrole.be/publications/avis-r%C3%A9glementation.
[14] Article 36 §1••, 1° de l'avant-projet.

2. À titre subsidiaire : discussion par article

1) L'article 15 de l'avant-projet

14. Le paragraphe 3, 5° de l'article 15 de l'avant-projet dispose que les services d'inspection peuvent à tout moment requérir l'assistance des services de la police fédérale ou locale dans l'exercice de leur mission de contrôle.

Le COC n'est pas en mesure de déterminer si l'auteur de l'avant-projet s'est concerté avec les corps de police réguliers des services de police au sujet de cette attribution de missions additionnelles aux services de police. Cette disposition aura un impact sur la capacité (et donc aussi sur les traitements d'informations et de données à caractère personnel effectués par les services de police) des corps concernés de la GPI, de sorte qu'il est recommandé de consulter les services de police et/ou leur autorité de tutelle à ce sujet.

Cette assistance n'est d'ailleurs nulle part détaillée dans l'avant-projet. De quel type d'assistance s'agit-il ? Une assistance dans le cadre des constatations ? Une assistance dans le cadre de l'enquête d'information? Le fait de prêter main forte au sens de l'article 44 de la LFP? Cette assistance supposera-t-elle certains actes policiers ayant un impact sur la gestion de l'information de la GPI? L'auteur de l'avant-projet est prié de faire la clarté sur ce point. Si l'objectif est seulement de prévoir une assistance telle que visée à l'article 44 de la LFP (comme par exemple l'assistance à un huissier de justice), il est indiqué de le préciser *expressis verbis* dans le texte de l'avant-projet.

2) L'article 36 de l'avant-projet

15. L'article 36 de l'avant-projet définit les principes, la base légale et les finalités du traitement de données à caractère personnel. Le paragraphe 1er, alinéa 1er commence comme suit :

l'échange d'informations entre l'autorité [de certification de cybersécurité] visée à l'article 5, §1er, l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, les autorités judiciaires, les autorités sectorielles ou les services d'inspection visés respectivement 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, les autorités de surveillance de marché, l'autorité nationale d'accréditation, les services de sécurité publique, les services de police, les services de renseignement et l'autorité visée à l'article 7, §4 de la du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique1[15] ;

Cette phrase peut prêter à confusion et créer un manque de clarté étant donné que l'on pourrait conclure de cette formulation que l'échange mutuel d'informations est également possible entre deux autorités autres que l'autorité de certification de cybersécurité. Or, on peut déduire de l'esprit des

[15] Soulignement et ajout entre crochets du COC.

articles que l'avant-projet vise uniquement l'échange d'informations entre l'autorité de certification de cybersécurité elle-même et une autre autorité. Toutefois, il serait préférable de l'indiquer plus clairement dans le texte de la loi. C'est le cas par exemple au point 2° du même article, à savoir: *« l'échange d'informations entre l'autorité [de certification de cybersécurité] d'une part et* (énumération des autorités publiques) *d'autre part».* La même confusion pourrait naître de l'article 6 §3 de l'avant-projet.

3) L'article 38 de l'avant-projet

16. L'article 38 de l'avant-projet, enfin, prévoit une dérogation à l'obligation de conclure un protocole pour le transfert de données à caractère personnel lorsque certaines conditions cumulatives sont remplies.

Le paragraphe 1er de cet article commence comme suit : *« 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 personne les* (énumération des autorités publiques) *ne doivent pas formaliser, par un protocole, ... »*[16]. Cette formulation fait par conséquent uniquement référence au Titre 1er de la loi sur la protection des données. Dans l'hypothèse où les services de police transmettront des données policières à l'autorité de certification de cybersécurité, le Titre 2 de la LPD est également d'application en l'occurrence. Il ne s'agit donc pas uniquement d'une dérogation à l'article 20 de la LPD.

Le Titre 2 de la loi sur la protection des données interdit le transfert de données à caractère personnel à d'autres fins que celles prévues au Titre 2, sauf si ce traitement ultérieur est autorisé par la loi[17]. L'article 44/11/9 de la LFP permet le transfert d'informations sous certaines conditions, dont l'obligation de conclure un protocole d'accord en cas de communication récurrente ou volumineuse de données à caractère personnel ou informations. Le COC renvoie à cet *effet* aux points 9 à 13 inclus. Contrairement à l'article 20 de la LPD, la LFP ne prévoit pas la possibilité de déroger à cette obligation par le biais d'une loi.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de donner suite aux remarques susmentionnées.

Avis approuvé par l'Organe de contrôle d l'information policière le 19/01/2022.

[16] Soulignement du COC.
[17] Article 29 §2 de la LPD.

CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uwkenmerk	Ons kenmerk	Bijlage(n)	Datum
/	DA210031		19.01.2022

Betreft: Advies betreffende het Voorontwerp van wet inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit.

Het Controleorgaan op de politionele informatie (hierna het 'COC' of 'het Controleorgaan'),

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (B.S.,* 5 september 2018, hierna afgekort ais 'WGB'), inzonderheid het artikel 59 §1, 2de lid, artikel 71 en Titel VII, inzonderheid artikel 236;

Gelet op de wet van 3 december 2017 *totoprichting van een Gegevensbeschermingsautoriteit(hierna* afgekort 'WOG');

Gelet op de wet van 5 augustus 1992 *op het politieambt(hierna* 'WPA');

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna *LED);*

Gelet op de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;

Gelet op het verzoek van 30 november 2021 van de eerste minister;

Gelet op het feit dat de Gegevensbeschermingsautoriteit het verzoek op 7 december 2021 heeft doorgestuurd naar het Controleorgaan;

Gelet op het verslag van de heer Koen Gorissen, lid-raadsheer in het Controleorgaan;

Brengt op 19 januari 2022 het volgend advies uit.

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en de omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2], heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid van de organieke wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (hierna 'WOG') bepaalt dat de competenties, taken en bevoegdheden ais toezichthoudende autoriteit bedoeld door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan. Dat betekent met name dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die niet onder de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of HR-verwerkingen. Het Controleorgaan moet worden geraadpleegd in het kader van de voorbereiding van wetgeving of een regelgevende maatregel betreffende de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikelen 59 §1, 2de lid en 236 § 2 van de WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn Politie-Justitie). In dit kader heeft het Controleorgaan ais opdracht om na te gaan of de door de politiediensten beoogde verwerkingsactiviteit in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en van Titel 2 (voor de operationele verwerkingen) van de WGB[4]. Bovendien heeft het COC ook een opdracht van advies uit eigen beweging, zoals bepaald in artikel 236, § 2, van de WGB, en een opdracht van algemene informatieverstrekking aan het grote publiek, de betrokkenen, de verwerkingsverantwoordelijken en de verwerkers op het gebied van het recht op bescherming van de persoonlijke levenssfeer en gegevensbescherming, zoals bepaald in artikel 240 van de WGB.

2. Met betrekking tot in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan uit eigen beweging of op verzoek van de regering of de Kamer van Volksvertegenwoordigers, een bestuurlijke of gerechtelijke autoriteit of een politiedienst advies uit over elke aangelegenheid die verband houdt met het beheer van politionele informatie, zoals bepaald in afdeling 12 van hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene

---

[1] 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 (hierna de 'Algemene Verordening Gegevensbescherming' of **'AVG'** genoemd).
[2] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (hierna de 'Richtlijn Politie en Justitie' of *LED (Law Enforcement Directive)* genoemd).
[3] Artikel 4 §2, 4de lid WGB.
[4] Artikel 71 §1, 3de lid WGB.
[5] Artikelen 59 §1, 2de lid en 236, §2 van de WGB.

Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BEL-PIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de WGB en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die krachtens of door andere wetten aan het Controleorgaan wordt verleend[6].

4. Het Controleorgaan is tot slot ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 inzake douane en accijnzen, zoals gewijzigd door de wet van 2 mei 2019 tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

II. Voorwerp van de aanvraag

S. De eerste minister richtte op 30 november 2021 een adviesaanvraag aan de Gegevensbeschermingsautoriteit met betrekking tot een voorontwerp van wet inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (hierna *'voorontwerp?-*

6. Bij toepassing van artikel 54/1 WOG stuurde de Gegevensbeschermingsautoriteit de aanvraag op 7 december 2021 door naar het Controleorgaan op de politionele informatie opdat dit laatste een advies zou uitbrengen over het voorontwerp.

7. Het Controleorgaan wijst erop dat de autoriteiten evenals de verwerkingen van persoonsgegevens en van informatie die exclusief onder zijn bevoegdheid ressorteren, strikt worden gedefinieerd door de wet en dat het zijn adviezen bijgevolg beperkt tot de verwerkingen die tot zijn bevoegdheid behoren, i.e. de verwerkingen die worden uitgevoerd door de politiediensten.

8. De adviezen van het COC blijven echter niet noodzakelijk beperkt tot het (de) artikel(en) zoals vermeld in een adviesaanvraag. Het COC houdt immers steeds rekening met alle elementen en bepalingen die tot zijn bevoegdheid behoren krachtens bovenvermelde regelgeving.

In dit geval betekent dit dat de artikelen 6, 15, 36, 38 van het voorontwerp worden geanalyseerd in het huidige advies.

III. Analyse van de aanvraag

[6] Artikel 71, §1, derde lid *Jundo* artikel 236, §3 van de WGB.

1. In hoofdorde

9. Het voorontwerp geeft uitvoering aan de Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de cyberbeveiligingsverordening) en regelt de bevoegdheden van de inspectiediensten, de sanctieregels, de klachten- en beroepsprocedures, de wettelijke machtigingen voor bepaalde delegaties, de algemene onafhankelijkheidsregels, enz. Het voorontwerp laat ook onderlinge informatie-uitwisseling toe tussen de cyberbeveiligingscertificeringsautoriteit en andere autoriteiten. Indien de informatie persoonsgegevens betreffen worden de modaliteiten ervan geregeld in hoofdstuk 8 van dit voorontwerp[7].

10. De cyberbeveiligingscertificeringsautoriteit kan persoonsgegevens uitwisselen met andere autoriteiten [8] (waaronder ook politiediensten), noodzakelijk om te voldoen aan de wettelijke verplichtingen van de cyberbeveiligingsverordening, van dit voorontwerp, of om een taak van algemeen belang te vervullen die is opgedragen aan een van de in dit voorontwerp bedoelde overheden.

De persoonsgegevens die kunnen uitgewisseld worden op basis van het voorontwerp, zijn meer bepaald identificatie- of authenticatiegegevens en elektronische communicatiegegevens van de volgende categorieën van personen:

Iedere persoon die optreedt voor:

- conformiteitsbeoordelingsinstanties,
- houders van Europese cyberbeveiligingscertificaten,
- afgevers van EU-conformiteitsverklaringen,
- een overheid;

Iedere persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten van de cyberbeveiligingscertificeringsautoriteit;

Iedere persoon die een klacht indient.

Het voorontwerp voorziet dus in gegevensoverdrachten tussen de nationale cyberbeveiligingscertificeringsautoriteit (i.e. federale overheid) en politiediensten.

11. Bij het versturen van informatie met de politiediensten moeten bepaalde wettelijke voorwaarden in acht worden genomen. Om de conformiteit ervan te analyseren, moet er in de eerste plaats worden nagegaan of het doorsturen van informatie in het kader van het voorontwerp eenzijdig of wederzijds is.

---

[7] Artikel 6, §3 Voorontwerp.

[8] Autoriteiten opgesomd in artikel 36, §1 van het voorontwerp.

Overeenkomstig het voorontwerp zal er politionele informatie worden doorgestuurd van de politiediensten naar een federale overheid, aangezien informatie-uitwisseling mogelijk zal zijn (zie punt 10).

Deze gegevensdoorgifte moet een wettelijke grondslag hebben, noodzakelijk zijn en in verhouding staan [9]. Voorde politiediensten is deze wettelijke grondslag te vinden in artikel 44/11/9 van de wet op het politieambt ('WPA'). Dit kan ook de toestemming van het openbaar ministerie zijn op basis van zijn prerogatieven[10].

12. Artikel 44/11/9 WPA regelt de mededeling van persoonsgegevens en informatie door de politiediensten. Paragraaf 2 ervan bepaalt: *"Overeenkomstig de nadere rege/s vastge/egd in de richtlijnen van de ministers van Binnenlandse Zaken en Justitie, elk in het kader van hun bevoegdheden, kunnen ze1[11] eveneens meegedeeld worden aan de Belgische openbare overheden, publieke organen of instellingen of instellingen van openbaar nut die door de wet belast zijn met de toepassing van de strafwet of die wettelijke verplichtingen inzake de openbare ve11igheid hebben, wanneer deze ze nodig hebben voor de uitoefening van hun wette/ijke opdrachten."*

Artikel 44/11/9 paragraaf 2 WPA verwijst naar een lijst die een volledige opsomming moet bevatten van overheden, organen of instellingen aan dewelke de politiediensten persoonsgegevens en informatie mogen meedelen. Overeenkomstig artikel 44/11/9 moet deze lijst worden vastgesteld door de ministers van Binnenlandse Zaken en Justitie, op basis van een voorstel van het Comité Informatie en ICT, na advies van het Controleorgaan. Op het ogenblik van opmaak van dit advies, heeft het Controleorgaan geen voorstel/adviesaanvraag van het voornoemde Comité ontvangen en bestaat deze lijst niet.

Bovendien vereisen de bepalingen van de WPA een protocolakkoord in geval van herhaalde of volumineuze mededeling van persoonsgegevens of informatie[12].

Bijgevolg voldoen deze doorgifte en de inhoud ervan, zoals bedoeld in het voorontwerp, niet aan de bepalingen van artikel 44/11/9 WPA[13].

13. Wat betreft de mededeling van informatie afkomstig van de nationale Cyberbeveiligingscertificeringsautoriteit aan de politiediensten bepaalt de auteur van het voorontwerp dat de persoonsgegevens "onderling" kunnen worden uitgewisseld[14]. De uitwisselingen van informatie tussen de federale autoriteit en de politiediensten verlopen dus in twee richtingen.

---

[9] Artikel 29, §1 WGB.
[10] artikel 21bisWetboek van Strafvordering en artikel 1380 Gerechtelijk Wetboek.
[11] Het betreft de persoonsgegevens en de informatie.
[12] Artikel 44/11/9, §2, lid **2 WPA.**
[13] Zie ook het advies van het COC betreffende het voorontwerp van decreet van 6 mei 2019 betreffende milieudelinquentie en diverse andere decreten (DA210008), 21 mei 2021, Adviezen/regelgeving I Controleorgaan op de oolitionele informatie.
[14] Artikel 36, §1, 1° Voorontwerp.

Overeenkomstig artikel 44/11/9, paragraaf 4 WPA dienen de nadere regels betreffende deze mededeling in een goedgekeurd protocolakkoord nader bepaald te worden.

2. In ondergeschikte orde: artikelsgewijze opmerkingen

1) Artikel 15 voorontwerp

14. Paragraaf 3, 5° van artikel 15 van het voorontwerp bepaalt dat de inspectiediensten op elk ogenblik bijstand mogen vorderen van de federale of lokale politiediensten bij de uitoefening van hun toezichthoudende opdracht.

Het is het COC niet duidelijk of deze toebedeling van bijkomende opdrachten aan de politiediensten door de steller van het voorontwerp werd overlegd met de reguliere politiekorpsen van de politiediensten. Deze bepaling zal een impact hebben op de capaciteit (en dus ook op de verwerkingen van informatie en persoonsgegevens door de politiediensten) van de betrokken korpsen van de GPI zodat het aanbeveling verdient één en ander te overleggen met de politiediensten en/of hun voogdijoverheid.

Deze bijstand wordt in het voorontwerp overigens niet nader gedetailleerd. Wat soort van bijstand bedoelt men? Bijstand bij de vaststelling? Bijstand bij de opsporing? Het verlenen van de sterke arm in de zin van artikel 44 WPA? Zal deze bijstand bepaalde politionele handelingen veronderstellen met impact op de informatiehuishouding van de GPI? De steller van het voorontwerp wordt verzocht hierin duidelijkheid te verschaffen. Indien het enkel de bedoeling is bijstand te voorzien zoals bedoeld in artikel 44 WPA (zoals bijv. de bijstand aan een gerechtsdeurwaarder) verdient het aanbeveling dit ook zo *expressis verbis* in de tekst van het voorontwerp op te nemen.

2) Artikel 36 voorontwero

15. Artikel 36 van het voorontwerp regelt de beginselen, de wettelijke basis en doeleinden van de verwerking van persoonsgegevens. Paragraaf 1, lid 1 begint ais volgt:

informatie-uitwisseling tussen de [cyberbeveiligingscertificeringslautoriteit bedoeld in artikel 5, § 1, de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, de gerechtelfjke overheden, de sectorale overheden of de inspectiediensten respectievelfjk bedoeld 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, de markttoezichtautoriteiten, de nationale accreditatieautoriteit, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7

april 2019 tot vaststelling van een kader voor de bevei/iging van netwerk- en informatiesystemen van algemeen belang voor de openbare veilighed1[15]*;*

Deze zin kan leiden tot onduidelijkheid en verwarring aangezien uit deze formulering kan geïnterpreteerd worden dat informatie-uitwisseling tussen twee autoriteiten, andere dan de cyberbeveiligingscertficeringsautoriteit, onderling ook mogelijk is. Uit de ratio van de artikels kan afgeleid worden dat enkel informatie-uitwisseling bedoeld wordt tussen de cyberbeveiligingscertificeringsautoriteit zelf en een andere autoriteit. Toch zou dit duidelijker kunnen weergegeven worden in de tekst van de wet. Dit wordt bijvoorbeeld wel gedaan in het ten 2° van hetzelfde artikel, namelijk ais volgt: *"informatie-uitwisseling tussen de [cyberbeveiligingscertificerings]autoriteit enerzijds en* (opsomming overheden) *anderzijds'*. Dezelfde verwarring zou kunnen ontstaan in artikel 6, §3 van het voorontwerp.

3) Artikel 38 voorontwerp

16. Tot slot, voorziet artikel 38 van het voorontwerp in een afwijking op de verplichting om een protocol te sluiten bij doorgifte van persoonsgegevens, indien aan bepaalde cumulatieve voorwaarden wordt voldaan.

Paragraaf 1 van dit artikel begint ais volgt: *"In afwiiking van artike/ 20 van de wet van 30 iu/i 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de vetwerking van persoonsgegevens moeten de* (opsomming overheden) *niet formaliseren aan de hand van een protocot ...*[16]*,* Er wordt bijgevolg enkel verwezen naar Titel Ivan de Wet gegevensbescherming. In de veronderstelling dat de politiediensten politionele gegevens zullen doorgeven aan de cyberbeveiligingscertificeringsautoriteit is Tite! II van de WGB hier ook op van toepassing. Dit houdt dus niet louter een afwijking in van artikel 20 WGB.

Tite! II van de Wet Gegevensbescherming verbiedt de doorgifte van persoonsgegevens voor een ander doeleinde dan voorzien in Titel II, tenzij deze verdere verwerking is toegestaan bij wet[17]. Artikel 44/11/9 WPA laat doorgifte van informatie toe onder bepaalde voorwaarden, waaronder de verplichting om een protocolakkoord te sluiten in geval van herhaalde of volumineuze mededeling van persoonsgegevens of informatie. Hiervoor verwijst het COC naar punt 9 tot en met 13. In tegenstelling tot artikel 20 WGB voorziet de WPA geen mogelijkheid am bij wet af te wijken van deze verplichting.

OM DEZE REDENEN,

Het Controleorgaan op de politionele informatie

[15] Onderlijning en toevoeging tussen vierkante haakjes door het COC.
[16] Onderlijning door het COC.
[17] Artikel 29, §2 WGB.

verzoekt de aanvrager gevolg te geven aan de hogervermelde opmerkingen.

Advies goedgekeurd door het Controle orgaan op de Politionele Informatie op 19/01/2022.

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 08/2022 du 21 janvier 2022

Objet : Avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (CO-A-2021-256)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité ») ; Présent.e.s. :Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA ») ;

Vu 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* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis du Premier Ministre, Alexander De Croo, reçue le 30 novembre 2021 ;

Vu les informations complémentaires reçues en date du 14 décembre 2021 ;

Émet, le 21 janvier 2022, l'avis suivant :

I. Objet et contexte de la demande

1. En date du 30 novembre dernier, le Premier Ministre a sollicité l'avis de l'Autorité sur l'avant-projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (ci-après « l'avant-projet de loi »).

2. Cet avant-projet de loi vise à exécuter le Règlement (UE) 2019/881 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 (TIC) (ci-après le « Règlement cybersécurité »).

3. Ce Règlement cybersécurité vise à renforcer la confiance dans le secteur des TIC en définissant un cadre européen de certification de cybersécurité, qui fixe des règles horizontales pour le développement de schémas de certification de cybersécurité pour différentes catégories de produits[1], services[2] et processus[3] TIC. L'ENISA a la charge de la préparation des schémas de certification qui seront ensuite adoptés par la Commission européenne au moyen d'actes d'exécution. Un schéma européen de certification de cybersécurité est, selon le Règlement Cybersécurité, « *un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC ou processus TIC spécifiques* ». Chaque schéma de certification spécifiera, entre autres, le type ou les catégories de produits, services et processus TIC couverts, l'objet, les normes et les méthodes d'évaluation. Les certificats de cybersécurité européen, délivrés par les organismes d'évaluation de la conformité accrédités par les organismes nationaux d'accréditation, attesteront qu'un produit TIC, service TIC ou processus TIC a été évalué en qui concerne sa conformité aux exigences de sécurité spécifique fixées dans un schéma européen de certification de cybersécurité. Le Règlement cybersécurité définit 3 niveaux d'assurance, qui sont corrélés à des niveaux de risques différents. Il s'agit des niveaux suivants : élémentaire, substantiel et élevé.

4. Sauf disposition contraire du droit de l'Union européenne ou du droit national d'un État membre, une certification ou une déclaration de conformité est volontaire. La Commission européenne évaluera à des intervalles planifiés la nécessité de rendre des certificats obligatoires. Le Règlement cybersécurité prévoit la possibilité de se faire certifier ou de procéder à une déclaration de

[1] Définis par le Règlement cybersécurité comme étant un *« élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information »*.

[2] Définis par le Règlement cybersécurité comme étant un « *service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information* ».

[3] Définis par le Règlement cybersécurité comme étant un « *ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance* ».

conformité. Un certificat est délivré par un organisme d'évaluation de la conformité indépendant et accrédité. Une déclaration de conformité est délivrée sous la responsabilité du fabricant ou fournisseur TIC au moyen d'une autoévaluation. Tout schéma de certification précise si une telle déclaration de conformité est permise ou pas et l'auto-évaluation est limitée au niveau d'assurance « élémentaire ».

5. Les Etats membres doivent en exécution de ce Règlement désigner la ou les autorités nationales de certification de cybersécurité, qui délivreront des certificats, ou encore qui assurent la supervision et le contrôle de la bonne application des règles par les différents acteurs (fabricants, fournisseurs et prestataires de produits et services TIC titulaires d'un certificat ou ayant émis une déclaration de conformité et organismes d'évaluation de la conformité). De plus, les Etats membres doivent définir des règles spécifiques dans leur droit national pour assurer la bonne application de ce Règlement, par exemple concernant les sanctions ou le retrait de certificats. C'est l'objet de l'avant-projet de loi soumis pour avis.

II. Examen

Observations générales – Communications de données par les autorités en charge du contrôle du respect du Règlement cybersécurité et des schémas européens de certification de cybersécurité et protection de la clientèle (personnes physiques) des prestataires de services ICT contrôlés (ou des clients personnes physiques de cette clientèle dont les données sont reprises dans les services ICT contrôlés)

6. Le présent avis de l'Autorité ne vaut que pour autant que des traitements de données concernant des personnes physiques soient visés par les dispositions de l'avant-projet de loi. Les traitements de données qui devront être réalisés dans le cadre des contrôles requis par le Règlement cybersécurité pourront porter sur des données à caractère personnel au sens du RGPD lorsque les fabricants ou fournisseurs de produits TIC, les prestataires de services TIC ou de processus TIC titulaires ou demandeurs d'un certificat de conformité de cybersécurité européen seront des personnes physiques mais également lorsque le contrôle du respect des schémas de certification par les prestataires desdits services TIC certifiés impliquera le traitement de données à caractère personnel telles que les données de leurs clients personnes physiques ou des clients personnes physiques de leurs clients. Si l'on prend, à titre d'exemple, des services cloud[4] ; il est fréquent que les clients d'un prestataire de service cloud l'utilisent pour leurs propres traitements de données à

[4] Cf EUCS, candidate cybersecurity certification scheme for cloud services, december 2020, disponible sur le site de l'ENISA à l'adresse suivante https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@@download/fullReport. Il y est prévu que « The EUCS scheme may cover any type of ICT service, provided that the ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface (ISO 17788) and that the ICT service aims at reaching the assurance level corresponding to one of the three levels « basic », « substantial » and « high » of the EUCSA as defined in the EUCS scheme.

caractère personnel ; lesquels peuvent porter sur des catégories particulières de données au sens du RGPD en fonction du domaine d'activité desdits clients (ex. un hôpital, un cabinet d'avocat ou encore une autorité publique en charge de mission de prévention et de détection d'infractions pénales).

7. Comme cela a été relevé par le Contrôleur européen à la protection des données dans un de ses avis récent sur la stratégie européenne en matière de cybersécurité et sur la directive SRI 2.0[5], « *l'article 5, paragraphe 1, point f), du RGPD a posé la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément l'obligation – applicable tant aux responsables du traitement qu'aux sous-traitants – de garantir un niveau de sécurité approprié. Ces deux dispositions indiquent clairement que la sécurité est essentielle au respect de la législation européenne en matière de protection des données. C'est pourquoi (…) l'amélioration de la cybersécurité est essentielle à la sauvegarde des droits fondamentaux. y compris du droit au respect de la vie privée et à la protection des données à caractère personnel (…). Dans le même temps, (…) la poursuite des objectifs de cybersécurité peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit* »

8. Au regard de ces considérations, l'avant-projet de loi est problématique en raison des échanges de données qu'il prévoit en des termes très larges entre, d'une part, l'autorité nationale de certification de cybersécurité et les autres autorités qui seront désignées pour la réalisation des missions de contrôle prévues par le Règlement cybersécurité et, d'autre part, les autorités suivantes: les autorités judiciaires, les autorités sectorielles ou les services d'inspection visés respectivement 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, les autorités de surveillance de marché, l'autorité nationale d'accréditation, les services de sécurité publique, les services de police, les services de renseignement et l'autorité visée à l'article 7, § 4 de la du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

[5] Avis du CEPD 05/2021 sur la stratégie en matière de cybersécurité et la directive SRI 2.0, disponible sur le site du CEPD à l'adresse suivante https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en

9. Ces échanges posent question au vu de leur objet très large, tel qu'actuellement prévus par l'avant-projet de loi. A plusieurs reprises, il y est en effet prévu qu'ils ont lieu non seulement pour l'exercice des missions de services public consistant au contrôle du respect du Règlement cybersécurité et des schémas de certification européen de cybersécurité ou des déclarations de conformité réalisées en exécution dudit Règlement mais également pour l'application de toute autre disposition légale (sans préciser de quelle disposition légale il s'agit ; ce qui ne permet pas de vérifier si elle présente un lien clair avec le Règlement cybersécurité précité). Cela apparait disproportionné, non conforme au champ d'application de l'avant-projet de loi censé mettre en œuvre le règlement cybersécurité, selon les considérations générales de l'exposé des motifs.

10. De plus, ce défaut d'encadrement minimal desdits échanges risque de mettre à mal l'objectif de confiance dans les produits et services TIC certifiés que poursuit le Règlement européen cybersécurité étant donné que les données des clients (ou de la clientèle de ceux-ci) des prestataires services TIC contrôlés par l'autorité de certification de cybersécurité pourront, selon le libellé de l'avant-projet de loi, être collectées et utilisées par des services publics qui ne disposent pas de mission spécifique liée à la cybersécurité tels que par exemple les services de police ou les services de renseignement et ce, pour leur propres missions de prévention et de détection de n'importe quelles infractions pénales, d'enquêtes et de poursuites ou encore pour n'importe quelles mission de la Sûreté de l'Etat et du service général du Renseignement et de la Sécurité. Cette situation risque de constituer un frein à la promotion de services et produits ICT certifiés conformément au Règlement cybersécurité et, par voie de conséquence, à l'amélioration de sécurité de l'information dans ces domaines.

11. L'auteur de l'avant-projet de loi doit donc encadrer les échanges conformément au strict nécessaire et raisonnable au regard du champ d'application et des objectifs du Règlement cybersécurité. L'article 58.7.a du Règlement cybersécurité prévoit d'ailleurs que c'est uniquement en coopération avec les « *autres autorités compétentes de surveillance du marché* » que les autorités nationales de certification de cybersécurité doivent superviser et faire respecter les règles prévues dans les schémas européens de certification de cybersécurité et non n'importe quelle autorité publique. L'article 58.7.h de ce Règlement prévoit quant à lui que les autorités nationales de certification de cybersécurité « *coopèrent avec d'autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC, et processus TIC des exigences du présent règlement ou des exigences de schéma de certification de cybersécurité spécifiques* ». Le considérant 102 de ce Règlement précise à ce sujet que « *la Commission devrait faciliter ce partage d'informations grâce à la mise à disposition d'un système général de soutien à l'information électronique, par exemple, le système d'information et de communication pour la surveillance des marchés (ICSMS) et le système européen d'échange rapide sur les produits*

dangereux (RAPEX) déjà utilisés par les autorités de surveillance du marché en vertu du Règlement (CE) n°765/2008. » Cet exemple de signalement des alertes quant à la présence d'un produit ou d'un service non conforme à un schéma de certification cadre bien avec le cadre européen de certification de cybersécurité tel que décrit à l'article 46 du Règlement de cybersécurité. Lesdits échanges doivent, aux yeux de l'Autorité, donc se limiter à la réalisation de cet objectif et ne pas permettre l'application de n'importe quelle disposition légale. Ce partage d'informations sur le non-respect, par des produits TIC, services TIC et processus TIC, des exigences du Règlement Cybersécurité ou de certains schémas européens de certification de cybersécurité spécifiques ne nécessite pas, selon l'Autorité, de devoir échanger les données à caractère personnel que lesdits clients mettent à dispositions desdits prestaires dans le cadre de leur relation contractuelle.

12. Interrogé quant à ce qui justifie la mise en place d'échange de données avec les différentes autorités visées à l'article 6, §3 en projet, le délégué du Ministre a précisé ce qui suit :
    a. En ce qui concerne les autorités judiciaires *: « il apparaît nécessaire que les autorités judiciaires puissent solliciter ou être notifiées des informations en cas d'infractions pénales (fraudes liées à la délivrance, aux contrôles, aux sanctions et aux réclamations des certifications de cybersécurité ou d'infractions pénales prévues par les différentes législations sectorielles - dont la loi NIS) ».* A ce sujet, l'Autorité relève, tout d'abord, qu'à la lecture de l'avant-projet de loi les infractions au Règlement cybersécurité et aux schémas européens de certification ne sont pénalisées que par la modification du Code de droit économique et que c'est le livre XV de ce Code qui organise déjà les communications de données que l'inspection économique peut réaliser dans l'exercice de ses missions. Ensuite, l'article 29 du Code d'instruction criminelle (Cicr) prévoit déjà que « toute autorité constituée, tout fonctionnaire ou officier public (…) qui, dans l'exercice de ses fonctions acquerra la connaissance d'un crime ou d'un délit, sera tenu de donner avis sur-le-champ au procureur du Roi près le tribunal dans le ressort duquel ce crime ou ce délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. ». Il n'est pas nécessaire, voir contre-productif en termes de protection des données à caractère personnel, de répéter sans la modaliser, cette communication de données dans l'avant-projet de loi ; d'autant plus que l'article 29 du Cicr impose le respect de certaines formalités à ce sujet. L'Autorité recommande par conséquent la suppression de cet échange de l'avant-projet de loi.

    b. En ce qui concerne les autorités sectorielles (NIS)[6] *: « ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle des mesures de sécurité des réseaux et*

[6] Ainsi qu'il ressort des informations complémentaires, il s'agit des autorités suivantes :

systèmes d'informations (P.S.I., voir article 21 et suivants de la loi NIS), qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant ».

A ce sujet, l'Autorité comprend que ces autorités sectorielles, disposant de missions spécifiques en matière de sécurité de l'information, doivent être informées que les organisations dont elles contrôlent le respect des dispositions de la loi précitée du 7 avril 2019 (dite loi NIS) utilisent des services ou produits TIC certifiés dont le non-respect du schéma de certification a été mis en évidence par l'Autorité nationale de certification ou une autorité désignée en exécution de l'article 5,§2 de l'avant-projet de loi. A ce sujet, l'Autorité se demande si les mesures de retrait de certification -qui devraient par nature être soumises à des mesures de publicité – ne devraient pas être suffisantes à cet effet. Si cela ne devait pas être le cas (ce qu'il convient de justifier dans l'exposé des motifs), vu la caractère lié à la cybersécurité des missions des autorités de contrôle instituées en vertu de la loi NIS, l'Autorité considère que ces échanges apparaissent nécessaires mais

---

« Les autorités sectorielles visées à l'article 3, § 3 de l'avant-projet de loi sont les autorités 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 (ci-après, « loi NIS »).

Il s'agit concrètement des autorités suivantes :

- *Désignées par la loi NIS :*
  - *La BNB (art. 95. de la loi NIS qui a inséré un article 36/47 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique).*
  - *La FSMA (art. 90 et 91 de la loi NIS ayant modifiés les art. 71 et 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers).*
  - *L'IBPT (art. 88. de la loi NIS qui a modifié l'art. 14, § 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges).*
- *Désignées par l'annexe 1 de l'arrêté royal du 12 juillet 2019 (portant exécution 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, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques) :*
  - *pour le secteur de l'énergie : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des transports :*
    - *En ce qui concerne le secteur du transport, à l'exception du transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
    - *En ce qui concerne le transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des fournisseurs de service numérique : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
- *Désignée par l'arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable :*
  - *le Comité national de sécurité pour la fourniture et la distribution d'eau potable »*

qu'il convient, en plus de définir la notion d' « *autorités sectorielles* » utilisée par l'avant-projet de loi (référence explicite aux autorités visées) et de déterminer clairement dans l'avant-projet de loi[7] les circonstances et modalités de ces communications de données par l'autorité nationale de certification de cybersécurité et les autorités désignées en exécution de l'article 5, §2 en projet ainsi que la finalité du traitement qui sera réalisé avec ces informations par lesdites autorités sectorielles. De plus, il conviendra alors aussi de prévoir la limitation des échanges relatifs au constat d'un manquement aux normes de sécurité de l'information dont ces autorités assurent le contrôle aux seules entités se trouvant sous la surveillance desdites autorités

c. En ce qui concerne les autorités de surveillance des marchés *: « Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle portant sur les mesures de sécurité appliquées par les entités sur lesquelles elles ont une compétence de contrôle, qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant. »*

Si ces autorités de surveillance des marchés disposent de missions spécifiques en matière de cybersécurité, ce qu'il appartient à l'auteur de l'avant-projet de loi de justifier, et si de telles communications quant à la certification des entités visées n'est pas déjà prévue par ailleurs, les communications visées apparaissent pertinentes et nécessaires mais il est renvoyé aux remarques précédentes sur les autorités sectorielles pour leur encadrement adéquat (désignation des seules autorités de surveillance disposant de telle compétence, limitation des échanges relatifs au constat d'un manquement aux normes de sécurité de l'information dont ces autorités de surveillance des marchés assurent le contrôle aux seules entités se trouvant sous la surveillance desdites autorités, …). A défaut, cette communication sera supprimée de l'avant-projet de loi.

d. En ce qui concerne les services de sécurité publique : *« Dans le cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou dans le cas où ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services.»*

[7] pour autant que ces précisions ne figurent pas déjà dans la loi NIS, ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier.

Interrogé quant aux autorités visées par cette notion de « *services de sécurité publique* », le délégué du Ministre a précisé qu'il s'agissait des autorités suivantes : *« SPF Intérieur, Bruxelles Prévention et Sécurité, Service public de Wallonie, Vlaamse Overheid, Administrations publiques locales (provinces et communes), Gouverneurs, OCAM ».*

Outre l'absence de définition dans l'avant-projet de la loi de la notion de service de sécurité publique (qu'il convient de pallier en se référant explicitement auxdites autorités ou plutôt, dans la plupart des hypothèses, à leur service compétent en matière de sécurité publique), le défaut d'encadrement minimal de ces échanges les rend non prévisibles. Ainsi qu'il ressort des informations complémentaires, il convient de les limiter aux hypothèses dans lesquelles une certification obligatoire a été imposée par lesdites autorités pour des motifs de sécurité publique et de prévoir que les mesures de retrait ou de suspension du certificat d'une entité (soumise à cette certification obligatoire) seront uniquement communiquées à l'autorité désignée dans la norme qui impose cette certification obligatoire. Cela, uniquement si des mesures de publicité quant au retrait d'un tel certificat pour non-respect du schéma de certification ne sont pas prévue ; ce qu'il convient de justifier dans l'exposé des motifs.

e. En ce qui concerne les services de renseignement *: « ils ont pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux menaces graves contre la sûreté de l'Etat. Lorsque cela s'avérerait nécessaire dans leurs recherches, par exemple lorsqu'une entité titulaire d'un certificat européen de cybersécurité aurait des liens avec des activités d'espionnage ou liées à une organisation criminelle, les services de renseignements devraient pouvoir avoir accès (en vertu de l'art. 14, al. 2 et art. 20, § 1er de la loi du 30 novembre 1998 sur les services de renseignement) aux informations collectées par le service d'inspection de l'autorité nationale de certification dans le cadre de ses missions de contrôle, au regard de l'importance de l'intérêt général protégé. En outre, dans la cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services. Faut encore qu'elles disposent de pouvoir d'investigation à ce sujet. »*

A ce sujet, en plus des considérations précédentes relatives aux mesures de publicité des retrait et suspension des certificats et à l'instar de la remarque faite en ce qui concerne les autorités judiciaires, l'Autorité considère qu'il n'est pas nécessaire, voir contre-productif

en terme de protection des données à caractère personnel, de répéter une communication de données au profit des services de renseignements qui est déjà encadrée par leur propre loi organique. De plus, cela sort du champ d'application de l'avant-projet de loi. Par conséquent, cet échange sera également supprimé.

f. En ce qui concerne les services de police : *« pour les mêmes motifs que ceux prévus pour les services de sécurité publique et les autorités judiciaires ».*

L'Autorité renvoie à ses remarques précitées faites à ce sujet.

13. Par conséquent, il convient de revoir le libellé des dispositions de l'avant-projet qui prévoient ces échanges (art. 6 §1 et 3, 7, 16 §2, 17 §1 et 3, 36, §1 et 3, 4° et 38) pour les rendre conformes aux considérations qui précèdent en les limitant à ce que requiert la réalisation des objectifs du Règlement cybersécurité ou de missions de services publics connexes touchant directement à la cybersécurité telles que celles poursuivies par les autorités de contrôle visées par la loi NIS (autorités sectorielles). L'auteur de l'avant-projet de loi veillera à ne pas prévoir des communications de données à caractère personnel qui sont déjà prévues par d'autres dispositions légales.

14. De plus, afin de préserver les droits et libertés des personnes physiques, clientes des prestataires contrôlés, potentiellement impactées par ces échanges, il est impératif d'insérer dans l'avant-projet de loi une disposition prévoyant que ces échanges ne peuvent pas porter sur des données à caractère personnel des clients personnes physiques (ou des clients personnes physiques de ces derniers) des prestataires de services ICT contrôlés au vu des risques importants que cela représente pour ces personnes concernées et étant donné qu'il ne ressort pas des justifications avancées par le délégué du Ministre que ces informations soient en l'espèce pertinentes et nécessaires.

15.

Enfin, au vu des objectifs du Règlement européen Cybersécurité, il importe que l'avant-projet de loi impose de manière explicite à l'Autorité nationale de certification de cybersécurité qui sera en charge du retrait des certificats une obligation d'information relative aux retraits de certificats intervenus. A cette fin, il convient d'imposer à cette Autorité de disposer d'un site web public et d'un service d'information (push) qui notifie à tous les acteurs concernés tout retrait de certification. Cela ne nécessite pas de communiquer des données à caractère personnel et cela cadre avec un des objectifs du Règlement européen Cybersécurité qui consiste à assurer la confiance dans les produits, services et processus TIC certifiés. Le cas échéant, une exception à cette publicité pourrait être envisagée pour des produits ou services TIC dont l'utilisation

nécessitent de disposer d'une habilitation de sécurité. D'un point de vue général, toute exception à la publicité des informations sur la révocation ou l'émission de certificats doit être prévue explicitement par l'avant-projet de loi et être dûment motivée et justifiée dans l'exposé des motifs.

Observations particulières

Champ d'application de l'avant-projet de loi

16. L'article 3 de l'avant-projet de loi détermine son champ d'application en précisant que la loi en projet s'appliquera à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement cybersécurité et que seuls les chapitres 1 à 4 et 7 et les articles 21 et 22 de cette loi en projet s'appliqueront aux certifications obligatoires.

17. Ainsi qu'il ressort des informations complémentaires, « *les mesures de contrôle et de sanctions liées aux certifications rendues obligatoires sont réglées ou devront être réglées par les différentes législations sectorielles applicables* ». Interrogé quant à la raison pour laquelle le chapitre 8 traitant des traitements de données à caractère personnel réalisés en exécution de la loi en projet avait été exclu des certifications européennes de cybersécurité obligatoires, le délégué du Ministre a précisé qu'il s'agissait d'un oubli et que ce chapitre 8 pouvait être inclus à l'article 3, §2 en projet. Il en est pris acte.

Désignation des autorités de contrôle compétentes

18. En exécution de l'article 58 du Règlement cybersécurité, l'article 5 de l'avant-projet de loi délègue au Roi le soin de désigner l'autorité nationale de certification de cybersécurité qui sera chargée des missions de contrôle et de supervision, visées à l'article 58 de ce Règlement. Le second paragraphe de cette disposition prévoit, à titre dérogatoire, que le Roi peut, « *en fonction du schéma de certification et à la demande de l'autorité publique concernée* », confier les missions de contrôle et de sanction (à l'exception du retrait et de la suspension des certificats) à une autre autorité publique. Interrogé à ce sujet, le délégué du Ministre a précisé que « *concrètement, il est envisagé d'utiliser éventuellement ce mécanisme au profit de l'IBPT, la FSMA, la BNB et l'inspection économique. Les dispositions modificatives ont été insérées dans le projet de loi à la demande de ces autorités car ces dernières considéraient les dispositions modificatives comme nécessaires pour que le Roi puisse éventuellement, dans les conditions imposées par la loi, les désigner.* »[8] Il en est pris acte.

[8] Au vu des désignation déjà effectuées par le biais des dispositions modificatives, l'Autorité s'interroge quant la nécessité de ces article 5, §2 en projet. Il est recommandé à l'auteur de l'avant-projet de loi de clarifier cela dans son avant-projet de loi. Dans la suite du projet d'avis, il sera référé à ces autorités de manière indifférenciée par la formulation « autorités désignées en exécution de l'article 5, §2 de l'avant-projet de loi ».

Coopération au niveau national (art. 6)

19. L'article 6 de l'avant-projet de loi traite des coopérations et échanges de données au niveau national que l'autorité nationale de certification de cybersécurité et les autorités publiques qui seront désignées en exécution de l'article 5, §2 en projet (pour l'exercice des missions visées aux chapitres 5 et 6 de l'avant- projet de loi) ainsi que d'autres autorités publiques réaliseront pour l'application du Règlement cybersécurité et de n'importe quelle autre disposition légale.

20. A ce sujet, il est renvoyé aux commentaires repris dans les observations générales du présent avis.

21. Si des collectes structurelles de données à caractère personnel doivent être réalisées par l'Autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 auprès de ces autorités sectorielles pour l'exercice des missions de service public prévues par le Règlement cybersécurité, elles doivent également être prévues dans l'avant-projet de loi et répondre aux mêmes critères de prévisibilité ; ce qui n'apparait pas être le cas actuellement.

22. Quant à l'article 6 § 2 en projet qui soumet les titulaires de certificat européens de cybersécurité et les émetteurs de déclaration de conformité à une obligation de communication, aux autorités en charge du contrôle du respect du règlement de cybersécurité et des schémas de certification européen, de toute information dont elles ont besoin dans l'exécution de leurs tâches, cette disposition en projet apparait redondante avec les dispositions de l'avant-projet de loi qui encadrent les pouvoirs d'inspection des services d'inspection de ces autorités et doit à ce titre être supprimée de cette partie de l'avant-projet de loi.

Echanges de données protégées par le secret professionnel ou par un devoir de confidentialité (art. 6, §4)

23. L'article 6, §4 en projet traite de la question des données protégées par le secret professionnel qui se posera dans le cadre des échanges de données que l'autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 en projet auront avec des tiers en ces termes :
« § 4. Les personnes dépositaires, par état ou par profession, 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, ainsi qu'éventuellement à d'autres autorités publiques lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.
Il s'agit notamment des informations nécessaires en matière de délivrance de certificats, de contrôle, de sanction et de réclamation. 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. »

24. Tout d'abord, l'Autorité ne perçoit pas en quoi la délivrance de certificats de sécurité nécessite de collecter des informations couvertes par le secret professionnel ou par un devoir de confidentialité. Selon l'exposé des motifs, seule la mission de contrôle est visée comme impactant potentiellement le secret professionnel et aucune justification quant à l'impact de la mission de délivrance de certificats de sécurité sur le secret professionnel ne ressort des informations complémentaires obtenues du délégué du Ministre. Par conséquent, à défaut de justification pertinente à ce sujet dans l'exposé des motifs, les termes « *délivrance de certificats* » seront omis de l'article 6, §4, al. 2.

25. Ensuite, l'Autorité relève qu'il y a, en matière d'échange de données protégées par le secret professionnel ou par un devoir de confidentialité, deux cas de figure qu'il convient de distinguer :
    a. tout d'abord, la situation dans laquelle se trouve une autorité soumise à un devoir de confidentialité qui se voit empêchée de communiquer des informations couvertes par ce devoir de confidentialité alors que lesdites communications sont légitimes, pertinentes et nécessaires (cf. supra) ;
    b. ensuite, la collecte, par les services d'inspection des autorités en charge du contrôle du respect du Règlement cybersécurité, de données à caractère personnel protégées par le secret professionnel (par exemple lors d'audit de systèmes ICT certifiés).

26. Ces deux situations doivent être appréhendées de manière distincte par l'avant-projet de loi et seule la première doit être abordée dans l'article 6 au vu de son intitulé (« *coopération au niveau national* »).

27. La disposition légale appréhendant le premier cas de figure (23.a) doit être de rédigée de manière telle que la levée de confidentialité ne peut avoir lieu qu'au profit d'autorités pour lesquelles les échanges de données sont légitimes[9], pertinents et nécessaires (cf. supra) pour l'exercice des devoirs d'inspection des autorités visées à l'article 5 de l'avant-projet de loi. De plus, le terme « *notamment* » à l'alinéa 2 du §4 de l'article 6 en projet doit être supprimé pour limiter correctement l'objet desdits échanges.

28. Quant au second cas de figure d'échange de données impactant le secret professionnel, c'est sous le chapitre traitant des pouvoirs d'inspection qu'il doit être appréhendé. Des garanties spécifiques pour les droits et libertés des personnes concernées par les données couvertes par ce secret professionnel doivent impérativement être prévues par l'avant-projet de loi de manière claire si et seulement si l'accès à de telles données est indispensable pour la réalisation des mesures

[9] En faisant référence à la disposition de l'avant-projet de loi qui décrira les modalités de ces échanges conformément aux observations de l'Autorité (cf. supra).

d'investigation du service d'inspection (autorisation préalable du juge d'instruction, intervention de l'Ordre professionnel auquel appartient la personne dont les documents devront être consultés pour la réalisation des contrôles précités sous peine de mettre en péril lesdits contrôles, interdiction de conservation de documents couverts par le secret professionnel par les autorités précitées,…cf. à ce sujet les articles 56bis et 90 octies du Code d'instruction criminelle). A défaut, il sera alors explicitement prévu que toute information couverte par le secret professionnel au sens de l'article 458 du Code pénal ne peut pas être collectée par le service d'inspection.

Chapitre 5 – Contrôle (art. 13 à 18)

29. Les articles 13 à 18 de l'avant-projet de loi encadrent la procédure de contrôle de l'autorité nationale de certification de cybersécurité et les pouvoirs dont disposera son service d'inspection.

30. L'article 13, §2 de l'avant-projet formalise les demandes d'informations que les inspecteurs pourront réaliser dans le cadre de leur mission, en ces termes :
« *Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande et précise le délai dans lequel les informations ou preuves doivent être fournies.* »

31. Afin que la personne contrôlée soit à même d'apprécier la pertinence et le caractère nécessaire des données (le cas échéant à caractère personnel) qui seront nécessaires dans ce cadre, il convient que cette disposition prévoie explicitement que les inspecteurs devront identifier les dispositions légales ou la ou les parties du schéma de certification auxquelles une infraction est suspectée.

Pouvoirs de contrôle du service d'inspection de l'autorité nationale de certification de cybersécurité – Mise en place de garanties pour la protection des données à caractère personnel reprises dans les systèmes informatiques audités

32. Les larges pouvoirs de contrôle du service d'inspection de l'autorité nationale de certification de cybersécurité sont décrits à l'article 15 de l'avant-projet de loi.

33. A l'instar de ce qui est prévu pour les perquisitions à l'article 15, §4 en projet, l'Autorité recommande d'ajouter dans l'avant-projet de loi des garde-fous pour les pouvoirs qui sont particulièrement intrusifs et qui permettront au service d'inspection d'avoir accès aux données à caractère personnel des clients (ou de la clientèle de ces derniers) des prestataires de services TIC ou fournisseurs de produits TIC qui seront contrôlés. A cet effet, au titre de garanties pour la préservation des droits et libertés des personnes concernées, il convient notamment d'interdire explicitement au service d'inspection de collecter ou de communiquer les données des clients (ou

de la clientèle de ces derniers) des prestataires et fournisseurs contrôlés pour des finalités autres que le contrôle du respect du règlement ou du schéma de certification concerné. Au même titre, l'Autorité considère qu'il convient de prévoir, à l'instar de ce qui est prévu à l'article 66 de la loi précitée du 7 avril 2019 (loi NIS), que, dès que des données à caractère personnel autres que celles concernant le titulaire du certificat européen ou les membres de son personnel doivent être accédées pour la réalisation des contrôles du service d'inspection, ces données doivent être, si possible, préalablement pseudonymisées selon les règles actuelles de l'art[10].

34. L'Autorité recommande également que le respect du principe de proportionnalité dans l'exercice des pouvoirs d'investigation soit explicitement inscrit dans l'avant-projet de loi, à l'instar de ce qui est fait pour d'autres pouvoirs d'inspection tels que ceux de l'inspection sociale (cf. code pénal social). Ainsi, il sera explicitement prévu, à l'article 15 de l'avant-projet de loi, que « lors de l'exécution de leurs pouvoirs de contrôle visés au présent article, les inspecteurs de l'autorité nationale de certification de cybersécurité et des autorités visées à l'article 5, §2 en projet veillent à ce que les moyens qu'ils utilisent soient appropriés et nécessaires pour le contrôle du Règlement cybersécurité ou des dispositions du schéma de certification dont ils contrôlent le respect ». Les collectes de données à caractère personnel qu'ils réalisent dans l'exercice de leurs missions de contrôle doivent se limiter aux seules données pertinentes pour prouver une infraction au règlement cybersécurité ou le non-respect d'un schéma de certification. Ils ne disposent d'ailleurs dans ce cadre pas d'autres pouvoirs que ceux-là.

35. Enfin, l'Autorité rappelle que l'opportunité de mener des investigations s'appréciera, dans le chef des inspecteurs, *in concreto,* au regard des éléments de fait à leur disposition. Ils disposent d'un pouvoir d'appréciation dans ce cadre. Les inspecteurs réaliseront les collectes électroniques de données nécessaires avec discernement et modération et n'accèderont à des données à caractère personnel que si, à la lumière des faits, ils disposent d'un faisceau d'indices concordants et sérieux que les données à caractère personnel recherchées rendraient possible ou accéléraient la prévention et la détection des infractions au Règlement cybersécurité ou au schéma de certification dont le respect est contrôlé.

Communication par le service d'inspection de ses rapports d'inspection et PV de contrôle à des tiers

36. L'article 16, §2 de l'avant-projet de loi prévoit que l'autorité nationale de certification de cybersécurité ou l'autorité désignée par le Roi en vertu de l'article 5, §2 de l'avant-projet de loi

[10] Cf à ce sujet ENISA : https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases et https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation;

communique une copie de son rapport d'inspection aux « *autorités de surveillance de marché, à l'autorité nationale d'accréditation, aux services de sécurité publique, aux services de police, au services de renseignement et à l'autorité visée à l'article 7,§4 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, à leur demande et pour autant que cela poursuive l'accomplissement de leurs missions légales*».

37. Pour les motifs évoqués sous les observations générales du présent avis, l'Autorité ne perçoit pas en quoi une telle communication sur simple demande s'avère opportune pour les services de renseignement, de sécurité publique et les services de police pour la bonne exécution du Règlement cybersécurité. Interrogé à ce sujet, le délégué du Ministre a précisé que « *la transmission d'une copie d'un rapport d'inspection ou d'un procès-verbal relatif au contrôle d'un certificat de cybersécurité par l'une des autorités précitées peut s'avérer nécessaire à l'exécution des missions légales de ces autorités ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique* » et a cité des dispositions légales existantes permettant à certaines autorités comme le Centre de crise nationale ou l'OCAM de disposer d'information de ce type. A ce sujet, l'Autorité relève tout d'abord que l'auteur de l'avant-projet de loi doit veiller à ne pas prévoir, en des termes flous, des flux de donnée qui sont déjà encadrés par d'autres dispositions légales. De plus, il ne rentre dans les objectifs de l'avant-projet de loi ni dans son champ d'application d'encadrer les pouvoirs d'inspection d'autres autorités publiques que celles qui sont chargées du contrôle du respect du règlement européen et des schémas de certification adopté en exécution dudit règlement. Ensuite, afin d'assurer la proportionnalité de cette disposition en projet, il convient de déterminer clairement dans l'avant-projet de loi les circonstances et finalités, légitimes et pertinentes pour l'exécution du Règlement européen cybersécurité, dans lesquelles lesdits rapports peuvent être communiqués aux seules autorités qui disposent de missions de service public spécifique en matière de cybersécurité et ce, en lieu et place de prévoir des communications sur simple demande sans autre précision et ce sans préjudice d'autres dispositions légales permettant à des autorités publiques d'accéder à certains rapport ou à certaines informations y reprises.

38. De plus, à l'instar de ce qui a déjà été recommandé, il convient de préciser que ces rapports ne peuvent contenir des données à caractère personnel concernant des clients (ou la clientèle de ces derniers) des prestataires de services ICT contrôlés au vu des risques que cela représente pour ces personnes concernées. Pour le surplus, l'Autorité renvoie à ses considérations générales reprises ci-dessus. Le libellé de l'article 16, §2 en projet devra être revu en conséquence.

39. L'article 16, §3 en projet détermine les destinataires auxquels ces rapports d'inspection devront être systématiquement transmis en cas de *« contrôle effectué auprès d'une infrastructure critique,*

d'un opérateurs de service essentiel ou d'un fournisseur de service numérique au sens 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 ou de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien ».

40. Ce faisant, l'avant-projet de loi instaure une obligation légale de traitement de données à caractère personnel (dans l'hypothèse où ces rapports contiendront des données à caractère personnel ou porteront sur un prestataire/fournisseur de service/produit ICT exerçant en personne physique) au sens de l'article 6.1.c du RGPD. Etant donné que les législations spécifiques visées à l'article 16, §3 en projet poursuivent un objectif similaire à celui du Règlement cybersécurité, l'Autorité n'a pas d'objection aux communications des rapports dans l'hypothèse où une inspection des autorités visées à l'article 5 de l'avant-projet de loi portent sur des entités utilisant lesdits services ou produits ICT visés par les législations mentionnées à l'article 16, §3. Par souci de sécurité juridique et de prévisibilité et par souci de conformité avec l'article 6.3 du RGPD, il convient toutefois de définir adéquatement la notion « *d'autorité sectorielle et de service d'inspection compétents* », de déterminer, à l'article 16, §3, la finalité précise pour laquelle ces rapports seront utilisés par ces autorités destinataires (à savoir, l'exercice de leurs missions de service public conférées par lesdites réglementations spécifiques) et de préciser que les rapports doivent être adressés uniquement à l'autorité sectorielle compétente en fonction du prestataire ou fournisseur de service ICT concerné par le rapport.

41. L'article 17 §1 à 4 de l'avant-projet détermine de manière très large la communication à des tiers de données et procès-verbaux de contrôle par le service d'inspection de l'autorité nationale de certification.

42. Le « *besoin d'en connaître en raison des missions poursuivies en lien avec la présente loi ou d'autres dispositions légales* » prévu à l'article 17, §1 en projet est un critère flou et trop large pour encadrer la communication de données à caractère personnel collectées par le service d'inspection à d'autres autorités d'autant plus que le §2 de cet article 17 en projet soumet le service d'inspection au secret professionnel. Par conséquent, cet article 17, §1 sera supprimé.

43. Quant à l'article 17, §3 en projet qui prévoit la communication par le service d'inspection de tout PV ou information complémentaire aux diverses autorités visées, l'Autorité renvoie aux remarques émises en observations générales dans le présent avis ainsi qu'aux remarques émises sur l'article 16, §2 en projet qui s'appliquent *mutatis mutandis.* De même, pour l'article 17, §4, il est renvoyé aux remarques émises sur l'article 16, §3.

Dérogation au principe de confidentialité des communications électroniques au profit du service d'inspection de l'autorité nationale de certification de cybersécurité

44. L'article 17, §5 en projet prévoit, en ces termes, une dérogation au principe de confidentialité des communications effectuées au moyen d'un réseau public et d'un service de communications électroniques accessibles au public[11] au profit du service d'inspection de l'autorité nationale de certification de cybersécurité:
« §. 5. Dans l'exercice de leurs fonctions, les membres du personnel du service d'inspection peuvent :
1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne leur est pas destinée personnellement ;
2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;
3° prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne. »

45. C'est dans les limites prévues à l'article 15 de la Directive ePrivacy que telles dérogations peuvent être prévues. L'article 15.1 de la Directive ePrivacy prévoit que : «*les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, […] et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne* »[12]. Avec l'entrée en vigueur du RGPD, il convient de lire l'article 15 de la Directive ePrivacy comme faisant référence à l'article 23 du RGPD. Cette disposition du RGPD prévoit notamment comme motif de limitation aux droits des personnes concernées « *l'exercice d'une mission de contrôle, d'inspection ou de réglementation liées, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a), b), c), d), e) et g) »* ; à savoir, notamment, la sécurité et la défense nationale, la sécurité publique, la prévention et détection d'infraction

[11] consacré par l'article 5.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite « Directive ePrivacy) implémenté en droit belge à l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques

[12] L'article 6 §§ 1 et 2 du traité sur l'Union européenne se lit comme suit : « 1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités […]. Il ressort de la jurisprudence de la CJUE que tous les causes de justification prévues à l'article 23 (ex 13 de la directive 95/46) du RGPD peuvent justifier une dérogation à ce principe de confidentialité des communications électroniques.

pénale, d'autres objectifs importants d'intérêts public général notamment un intérêt économique ou financier important et la prévention et détection de manquements à la déontologie de profession réglementée.

46. Il appartient tout d'abord à l'auteur de l'avant-projet de loi d'expliciter dans l'exposé des motifs en quoi la dérogation envisagée au profit du service d'inspection de l'autorité nationale de certification de cybersécurité cadre avec un ou plusieurs des motifs explicités à l'article 23.1 du RGPD.

47. Ensuite, au vu des motifs sur base desquels une dérogation à ce principe de confidentialité peut être prévue par les Etats membres, l'Autorité s'interroge s'il ne conviendrait pas en l'espèce de limiter ces dérogations aux contrôles qui seront opérés sur les organismes d'évaluation de la conformité ainsi que sur les titulaires de certificats obligatoires étant donné que c'est dans des domaines d'intérêt public important que des mesures législatives devraient être adoptées pour imposer de tels certificats. Il est indiqué que l'auteur de l'avant-projet de loi justifie sous cet angle le choix qu'il posera pour le champ d'application de la dérogation et insère sa justification dans l'exposé des motifs.

48. Interrogé quant aux besoins du service d'inspection nécessitant la mise en place d'une telle dérogation au principe de confidentialité des communications électroniques, le délégué du Ministre a précisé que « *ne sont pas visées les écoutes téléphoniques mais la* (prise de connaissance) *des e-mails émanant et reçus des organismes d'évaluation de la conformité, des émetteurs de déclaration de conformité, des titulaires de certificat de cybersécurité européen et ce uniquement lorsque les données en question sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification dont le respect est contrôlé* ».

49. Par conséquent, afin de garantir le caractère proportionné de la dérogation, il appartient à l'auteur de l'avant-projet de loi de préciser, à l'article 17, §3 en projet, que c'est uniquement les communications électroniques émanant et reçues des organismes d'évaluation de la conformité, (des émetteurs de déclaration de conformité)[13], des titulaires de certificat (obligatoire)[14] de cybersécurité européen que les inspecteurs pourront prendre connaissance et ce, uniquement si ces informations sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification (obligatoire) contrôlé ou au Règlement européen cybersécurité. Par souci de sécurité juridique et de prévisibilité, il sera aussi explicitement précisé que l'article 17, §3 déroge à l'article 124 de la loi précitée du 13 juin 2005.

[13] En fonction du choix qui devra être opéré au regard de la considération précédente.

[14] *Ibidem*

50. Enfin, interrogé quant à l'opportunité de prévoir des garanties pour les personnes contrôlées tel que leur accord préalable pour la consultation de leur communications électronique ou à défaut, l'accord du juge d'instruction, le délégué du Ministre a précisé que « *en l'absence du consentement expresse de l'entité contrôlée, les membres assermentés du service d'inspection de l'autorité nationale de certification de cybersécurité ne pourront pas prendre connaissance de ces informations (ceux-ci n'ayant pas la qualité d'officier de police judiciaire) ».* Il est donc indiqué de prévoir à l'article 17, §3 en projet que c'est après accord de la personne contrôlée que les consultations visées auront lieu.

Chapitre 8 – Traitement de données à caractère personnel

51. L'auteur de l'avant-projet de loi a opté pour l'insertion d'un chapitre spécifique dans son avant-projet visant à déterminer différents éléments des traitements de données à caractère personnel encadrés par l'avant-projet de loi.

Catégories de traitement de données à caractère personnel et finalités desdits traitements

52. L'article 36, §1er et 3 décrit les catégories de traitements de données à caractère personnel réalisés dans le cadre de l'exécution de la loi en projet en ces termes :
« *Art. 36. § 1er. Les traitements de données à caractère personnel effectués dans le cadre de l'exécution de la présente loi sont les suivants :*
1° l'échange d'informations entre l'autorité visée à l'article 5, § 1er, l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, les autorités judiciaires, les autorités sectorielles ou les services d'inspection visés respectivement 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, les autorités de surveillance de marché, l'autorité nationale d'accréditation, les services de sécurité publique, les services de police, les services de renseignement et l'autorité visée à l'article 7, § 4 de la du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
(…)
2° l'échange d'informations entre les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne, d'une part, et l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'autre part.
(…)
3° le traitement de données par l'autorité visée à l'article 5, § 1er ou par un organisme d'évaluation de la conformité, pour accomplir les tâches en matière de réclamation visées au chapitre 7.
(…) ;

4° le traitement de données par l'autorité visée à l'article 5, § 1er ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, relatives à ses tâches en matière de contrôle et de sanction.
(…)
§ 3. Les finalités pour lesquelles les traitements visés au paragraphe 1er sont effectués, sont les suivantes :
1° la délivrance de certificats de cybersécurité européens ;
2° la supervision des titulaires de certificats de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne ou des organismes d'évaluation de la conformité ;
3° le traitement des réclamations introduites sur base de l'article 63, § 1er du Règlement sur la cybersécurité ;
4° la coopération, en ce compris l'échange d'informations, au niveau national et international ;
5° l'imposition des sanctions prévues au chapitre 6. »

53. Tout d'abord, l'Autorité relève que la notion de « *traitements de données à caractère personnel effectués dans le cadre de l'exécution de la présente loi* » ne sert pas les exigences de prévisibilité. Au vu du champ d'application de l'avant-projet de loi, il convient d'encadrer uniquement les traitements de données à caractère personnel que réaliseront l'autorité nationale de certification de cybersécurité ainsi que le cas échéant les autorités désignées en exécution de l'article 5,§2 de l'avant-projet de loi (pour autant que ces derniers traitements ne sont pas déjà encadrés par les lois organiques de ces autorités) en exécution des missions de service public décrites au Règlement européen cybersécurité et que la loi en projet leur octroie. L'avant-projet de loi ne doit pas encadrer des traitements de données qui sortent de ce champ d'application ou qui sont par ailleurs déjà encadrés par les lois organiques d'autres autorités ; ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier.

54. Une description exhaustive des catégories de traitements de données réalisés en exécution de la loi en projet, tel que tente de le faire l'article 36, §1 en projet, risque de porter préjudice à l'exercice des missions de service public de l'autorité nationale de certification dans l'hypothèse où interviendrait un oubli. Une détermination claire et concrète des finalités des traitements de cette autorité (en plus de la détermination de leurs autres éléments essentiels) doit suffire à assurer la prévisibilité requise à ces traitements de données à caractère personnel. L'Autorité recommande la suppression de l'article 36, §1 en projet.

55. Quant à la détermination des finalités des traitements, faite à l'article 36, §3 en projet, il convient de viser les finalités pour lesquelles l'autorité nationale de certification et/ou les autorités qui seront désignés en exécution de l'article 5, §2 de l'avant-projet de loi traiteront des données à caractère personnel dans le cadre des missions de service public qui leur sont octroyées par

l'avant-projet de loi et le Règlement européen cybersécurité[15]. Les remarques suivantes s'imposent à ce sujet :

a. Les finalités visées à l'article 36, §3, 1° et 3° seront utilement fusionnées : délivrance des certificats de cybersécurité européen et gestion des réclamations y relatives ;
b. Les finalités visées à l'article 36, § 3, 2° et 5° seront également fusionnées et il sera fait référence aux dispositions pertinentes de l'avant-projet de loi en ces termes : contrôle des titulaires de certificat de cybersécurité européens, des émetteurs de déclarations de conformité de l'Union européenne et des organismes d'évaluation de conformité et le cas échéant imposition de sanction conformément aux chapitres 5 et 6 de la présente loi ;
c. Quant à la « coopération, en ce compris l'échange d'information au niveau national et international », il ne s'agit pas d'une finalité de traitement au sens du RGPD mais d'un traitement de données en soi qui doit être déjà couvert par les finalités de contrôle et de sanction précitées voir, si nécessaire et conforme au Règlement cybersécurité, par la finalité de « *délivrance des certificats* ». L'article 36, §3, 4° sera par conséquent supprimé et le cas échéant, si les dispositions législatives existantes (Loi NIS) ne prévoient pas déjà de manière prévisible lesdits flux, cette disposition en projet sera remplacée par la finalité concrète pour laquelle une communication d'informations sera réalisée par l'autorité nationale de certification et les autorités désignées en exécution de l'article 5, §2 en projet aux seules autorités sectorielles compétentes (NIS) et ce, conformément aux articles 16 et 17 de l'avant-projet de loi (adaptés conformément aux recommandations précitées de l'Autorité). De plus, si l'auteur de l'avant-projet de loi vise la participation de l'Autorité nationale de certification de cybersécurité à la coopération internationale en vue de l'amélioration de la qualité des certifications et l'harmonisation des approches en la matière et qu'une telle coopération nécessite un échange de données à caractère personnel entre les autorités nationales de certification de cybersécurité, il est indiqué de mentionner une telle finalité de manière concrète et précise.

Qualification du responsable du traitement

56. Afin d'éviter toute ambiguïté quant à l'identité de l'entité qui doit être considérée comme responsable du traitement et afin de faciliter ainsi l'exercice des droits de la personne concernée tels que prévus aux articles 12 à 22 du RGPD, l'Autorité invite l'auteur de l'avant-projet de loi à identifier plus explicitement que ce qu'il ne fait à l'article 36, §1 en projet le ou les responsables de traitement.

[15] L'article 36 en projet vise actuellement l'encadrement des « *traitements de données réalisé en exécution de la loi* » Or, tous les traitements de données réalisés pour la finalité de « *délivrance des certificats de cybersécurité européens* » ne sont, à juste titre, par couverts par l'avant-projet de loi. Le libellé de l'article 36 en projet sera donc revu sur ce point.

57. A cet effet, la précision selon laquelle l'autorité nationale de certification de cybersécurité est responsable des traitements qu'elles réalisent pour la réalisation des finalités visées à l'article 36, §3 suffit. Il en sera fait de même pour les autorités visées à l'article 5, §2 de l'avant-projet en ce qui concerne les traitements réalisés pour les finalités de contrôle et de sanction visées au chapitre 5 et 6 de l'avant-projet de loi.

Base de licéité

58. L'article 36, §2 en projet la base de licéité des traitements visés en ces termes
« § 2. Les traitements visés au paragraphe 1er sont nécessaires pour respecter les obligations légales découlant du Règlement sur la Cybersécurité ou de la présente loi, ou exécuter une mission d'intérêt public dont est investi l'une des autorités publiques visées par la présente loi. »

59. L'Autorité relève que la majorité des traitements de données à caractère personnel visés par la loi en projet seront des traitement réalisés par l'autorité nationale de certification de cybersécurité (et les autorités visées à l'article 5, §2 en projet) en exécution de ses missions de service public ; dont la base de licéité, au sens du RGPD, est l'article 6.1.e du RGPD (à l'exception des communications obligatoires systématiques de rapports et procès-verbaux d'inspection prévues aux articles 16, §3 et 17§4 de l'avant-projet de loi, dont la base de licéité est l'article 6.1.c du RGPD).

60. L'article 36, §2 en projet n'apporte aucune plus-value en termes de prévisibilité des traitements de données visés. Pour assurer la licéité et la prévisibilité des traitements qui se fondent sur l'article 6.1.e. du RGPD, une norme juridique nationale ou supranationale d'application directe doit déterminer de manière suffisamment claire et précise les missions de service public dont est investi le responsable du traitement (ce qui est le cas dans l'avant-projet de loi et le Règlement européen cybersécurité), mais il n'est pas requis que cette norme ou la norme nationale d'exécution d'un Règlement européen précise que les traitements de données effectués à cette fin le sont en «*exécution d'une mission d'intérêt public dont est investi le responsable du traitement* ». En conséquence, cet article 36, §2 en projet sera supprimé.

Catégories de données à caractère personnel traitées

61. L'article 36, §4 détermine, en ces termes, les catégories de données à caractère personnel traitées :
« § 4. Les données personnelles traitées sont des données d'identification ou d'authentification et des données de communications électroniques.

Le Roi peut, après avis de l'autorité visée à l'article 5, § 1er ou de l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, compléter l'alinéa précédent par d'autres données à caractère personnel. »

62. Outre le fait que l'avant-projet de loi ne précise pas par quelle entité ces catégories de données sont traitées, cette détermination ne présente pas de plus-value en termes de prévisibilité des traitements de données visés. De plus, en application du principe de légalité, l'Autorité considère qu'il ne peut en l'espèce être délégué au Roi le soin de compléter la liste des catégories de données à caractère personnel qui devront être traitées par l'Autorité nationale de certification de cybersécurité et les autorités désignées en application de l'article 5, §2 de l'avant-projet de loi pour la réalisation des missions de service public que l'avant-projet de loi leur confie. La liste actuelle étant manifestement lacunaire (quid des données relative à l'expertise ou à la formation du personnel du prestataire certifié ou en cours de certification ?...), il convient de la compléter au regard des critères communs (common criteria)[16] en la matière et son contenu doit être dûment justifié et motivé dans l'exposé des motifs.

63. En ce qui concerne les catégories de données traitées en application des chapitres 5 et 6 de l'avant-projet de loi (contrôle et sanction), l'Autorité reconnait qu'l n'est pas envisageable de les déterminer autrement que de manière fonctionnelle, en précisant qu'il s'agit des données nécessaires à l'exercice des missions de contrôle et de sanction visées aux chapitre 5 et 6 de l'avant-projet..

64. Par conséquent, l'article 36, §4 de l'avant-projet de loi sera revu en conséquence.

Catégories de personnes physiques à propos desquelles des données sont traitées

65. L'article 36 §5 détermine, en ces termes, les catégories de personnes à propos desquelles des données sont traitées pour la réalisation des finalités précitées :
« § 5. Les catégories de personnes dont les données à caractère personnel sont susceptibles de faire l'objet des traitements visés au paragraphe 1er sont les suivantes :
1° toute personne 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 ;

[16] Les Critères communs d'évaluation de la sécurité des technologies de l'information (appelés Critères communs ou CC) sont une norme internationale (ISO/IEC 15408) pour la certification de la sécurité informatique.

2° toute personne participant à un contrôle ou à une audition dans le cadre des missions de contrôle prévues au chapitre 5 ;
3° toute personne introduisant une réclamation. »

66. Tout d'abord, il convient de viser les personnes physiques et non simplement les personnes.

67. Ensuite, l'Autorité s'interroge quant au caractère éventuellement lacunaire de cette énumération au vu de ses observations générales reprises en début d'avis. Si tel est le cas, il convient d'y pallier et, au titre de garantie pour la préservation des droits et libertés des clients (ou de la clientèle de ces derniers) des prestataires des services/fournisseurs de produits ICT et conformément aux considérations générales de l'Autorité reprises en début d'avis, il importe de préciser que l'autorité nationale de certification de cybersécurité et les autorités désignées en application de l'article 5, §2 en projet, ne peuvent traiter des données concernant des personnes physiques clientes (ou la clientèle de ces dernières) des prestataires de services/fournisseurs de produits ICT contrôlés pour des finalités autres que le contrôle du respect par ces prestataires/fournisseurs du Règlement européen cybersécurité et des schémas européens de certification qui font l'objet du contrôle.

Durée de conservation

68. L'article 39 détermine la durée de conservation des données collectées en exécution de l'avant-projet de loi en ces termes :
« Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, visé à l'article 89 du Règlement UE 2016/679, les données à caractère personnel traitées en exécution de la loi sont conservées, sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. »

69. Comme déjà explicité ci-dessus, c'est la durée de conservation des données à caractère personnel collectées par l'autorité nationale de certification de cybersécurité et les autorités qui seront désignées en exécution de l'article 5, §2 en projet pour la réalisation des finalités visées à l'article 36, §3 qu'il convient de déterminer. La formulation de l'article 39 en projet sera utilement adaptée en ce sens.

70. En ce qui concerne la durée de conservation prévue, l'Autorité n'a pas de remarque à formuler.

Dérogation aux droits des personnes concernées

71. L'article 37 de l'avant-projet de loi déroge de manière très large à tous les droits des personnes concernées en vertu du RGPD.

72. Toute limitation aux droits dont disposent les personnes concernées en vertu du RGPD doit, non seulement, poursuivre un des objectifs énumérés à l'article 23.1 du RGPD, mais également répondre aux formes prescrites par l'article 23.2 du RGPD. De plus, toute limitation aux droits des personnes concernées se doit également d'être limitée au strict nécessaire tant en termes d'ampleur que de durée[17].

73. Tout d'abord, il convient de viser explicitement les responsables du traitement bénéficiant desdites dérogations, à savoir, ainsi qu'il ressort des informations complémentaires, l'autorité nationale de certification de cybersécurité et les autorités qui seront désignées en exécution de l'article 5, §2 en projet.

74. Selon l'article 37 en projet, les traitements desdits responsables qui bénéficieront de la dérogation envisagée sont ceux qui seront effectués pour la finalité de contrôle ainsi que pour la finalité de gestion des réclamations relatives à l'octroi d'un certificat de cybersécurité ou au refus de délivrance d'un tel certificat.

75. Bien que l'Autorité comprenne la nécessité de prévoir des dérogations à certains droits garantis par le RGPD pour les traitements de contrôle (pour ne pas mettre en péril ces opérations de contrôle), l'Autorité s'interroge quant à la nécessité de prévoir ce type de dérogation pour la gestion des réclamations relative à l'octroi ou au refus d'octroi des certificats. Pour ces derniers traitements, l'Autorité peut, par contre, comprendre la nécessité de prévoir dans l'avant-projet de loi la possibilité pour un plaignant de solliciter le traitement de sa réclamation de manière telle que son anonymat soit préservé (pour autant que la gestion de sa réclamation le permette) mais, outre cette hypothèse qui peut être prévue dans l'avant-projet de loi, il n'apparait pas nécessaire, au vu des informations complémentaires obtenues, de prévoir une dérogation au droits visés aux articles 12 à 22 du RGPD pour assurer le traitement adéquat des réclamations. A défaut de justification pertinente à ce sujet dans l'exposé des motifs, le champ d'application de la dérogation sera réduit en conséquence.

[17] Avis n° 34/2018 du 11 avril 2018 *concernant un avant-projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre 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* et plus spécifiquement ses considérants 36 à 38 ; Avis n° 41/2018 du 23 mai 2018 *concernant un avant-projet de loi portant des dispositions financières diverses* ; Avis n° 88/2018 du 26 septembre 2018 *sur le projet d'arrêté du Gouvernement flamand portant adaptation des arrêtés du Gouvernement flamand au règlement (UE).*

76. Ensuite, concernant la dérogation au profit des traitements de données réalisés par les services d'inspection aux fins d'exercice de leurs missions de contrôle prévue à l'article 13 de l'avant-projet de loi, l'Autorité relève que, en application de l'article 23.2 du RGPD, c'est à l'auteur de l'avant-projet de loi de préciser, à l'article 37 en projet, l'étendue des limitations introduites non seulement en terme de droits auxquels il est dérogé mais aussi en terme de limites de la dérogation prévue et ce, en lieu et place de prévoir que « *l'exemption ne vaut que si et dans la mesure où ces traitements sont nécessaires pour les finalités définies ci-avant, notamment dans la mesure où l'application des droits prévus par le règlement précité nuirait aux besoins d'un contrôle, d'une enquête ou d'une réclamation » ;* ce qui ne sert pas la sécurité juridique requise en la matière.

77. A ce sujet, sans viser à l'exhaustivité, l'Autorité recommande de préciser que les dérogations aux droits des personnes concernées ne sont d'application que pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (y compris les actes préparatoires de maximum 1 an après réception de la demande d'exercice du droit[18]) et pendant la période nécessaire en vue d'exercer les poursuites en la matière et ce, dans la mesure où l'exercice des droits nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires.

78. Quant au choix des articles du RGPD auxquels il est décidé de déroger dans l'avant-projet de loi pour l'exercice de la mission d'inspection, les remarques suivantes s'imposent :
    a. L'article 12 du RGPD explicite la transparence des informations et communication et modalités de l'exercice des droits des personnes concernées et ne constitue pas en soi un droit des personnes concernées. Il n'y a pas lieu d'y déroger.
    b. La nécessité de déroger au droit à l'effacement (art. 17 RGPD) pour l'objectif poursuivi n'apparait pas. Interrogé à ce sujet, le délégué du Ministre a précisé qu'« *il est prévu que les données à caractère personnel soient conservées sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. Cette durée se justifie par la nécessité de s'assurer de conserver plus longtemps les données à caractère personnel pouvant être liées à un faux ou usage de faux relatif à une certification de cybersécurité. Le service d'inspection doit également pouvoir d'identifier les cas de récidive pour les mêmes faits dans un délai de trois ans (qui peuvent donner lieu au doublement de l'amende administrative en vertu de l'article 24, § 4 de l'avant-projet). Or, sur base du droit à l'effacement, la personne concernée pourrait obtenir l'effacement prématuré de ses données. Il apparaît donc nécessaire de limiter ce droit* ». A ce sujet, l'Autorité relève que le droit à l'effacement ne permet pas à une personne concernée d'obtenir l'effacement de

[18] Afin d'assurer une limitation dans le temps raisonnable à la dérogation.

ses données de manière prématurée mais uniquement quand un des motifs visés à l'article 17 s'applique, ce qui n'apparait pas en l'espèce comme invalidant pour la procédure de contrôle du service d'inspection. Il convient d'ailleurs de relever que les services de l'inspection sociale et de l'inspection fiscale ne bénéficient pas non plus de dérogation à ce droit alors que les motivations de leurs dérogations aux droits des personnes concernées du RPGD sont les mêmes. Par conséquent, la dérogation à ce droit sera supprimée de l'article 37 en projet.

c. Dans le même ordre d'idées que ce qui précède, la dérogation au droit d'opposition sera également ôtée de l'article 37 en projet et ce, pour les mêmes motifs. L'article 21 du RPGD prévoit que lorsqu'une personne concernée s'oppose à un traitement de ses données qui est fait pour l'exercice d'une mission de service public, « *le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne prouve qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou la constatation, l'exercice ou la défense de droits en justice* » ; ce que l'autorité de certification n'aura pas de mal à prouver dans l'hypothèse où un tel droit est exercé par une personne contrôlée ; ce qui est d'ailleurs fort improbable étant donné qu'une personne concernée ne sait exercer ce droit que lorsqu'elle a connaissance d'un contrôle à son égard ; ce qui ne sera pas le cas étant donné qu'il est dérogé aux droits d'information et d'accès.

d. Quant à la dérogation à l'article 22 du RGPD faite par l'article 37 en projet, le délégué du Ministre a fait valoir à cet égard que « *des décisions individuelles automatisées (fondées sur l'utilisation d'algorithmes) en matière de contrôle et de sanctions ne sont pas prévues à ce stade mais leur utilisation pourrait s'avérer dans le futur utile ou nécessaire*. » Conformément à l'article 22.2 du RGPD, pour que les autorités visées à l'article 5 de l'avant-projet de loi puissent adopter des décisions fondées exclusivement sur un traitement automatisé produisant des effets juridiques sur la personne concernée ou l'affectant de manière significative, lesdites décisions doivent être prévues par une disposition législative spécifique qui doit encadrer lesdites décisions automatisées et prévoir des mesures appropriées pour la sauvegarde des droits et liberté et des personnes concernées ; ce qui n'est pas le cas de l'avant-projet de loi soumis pour avis. Par conséquent, la dérogation à l'article 22 du RGPD n'apparait pas nécessaire et doit également être omise.

e. Il convient également d'ôter l'article 20 du RGPD de la liste des articles auxquels il est dérogé étant donné qu'il n'est de toute façon pas d'application en l'espèce, ce qui a été confirmé par le délégué du Ministre.

79. De plus, pour rendre l'article 37 en projet compatible avec l'article 23.2 du RGPD, il convient de prévoir des garanties similaires à ce qui est prévu au chapitre 5/1 du code pénal social, lesdites dérogations et les garanties pour les droits et libertés des personnes concernées ayant déjà été approuvées par l'autorité de protection des données[19] (association du délégué à la protection des données autorités visées à l'article 5 en projet pour la consignation des motifs de fait ou de droit sur lesquels se fonde la décision de refus d'accéder au droit de la personne concernée et mise à disposition desdits motifs à l'Autorité de protection des données à 1ère demande, information des personnes concernées du refus d'accéder à sa demande et des motifs sauf si cela risque de compromettre la finalité de contrôle, information des personnes concernées ayant souhaité exercer leurs droits de la levée de la dérogation dès la clôture du contrôle, information des personnes concernées des recours dont elles disposent dans ce cadre, …).

80. L'Autorité ne perçoit pas la pertinence de l'article 37, §4 en projet. Il ne sert par ailleurs pas la sécurité juridique requise en matière de dérogation à un droit fondamental. Sa suppression est recommandée.

81. L'article 37, §5 sera également supprimé étant donné qu'il est redondant par rapport à d'autres dispositions de l'avant-projet de loi et sans lien avec les exigences de l'article 23.2 du RGPD.

Dérogation à l'article 20 de la LTD

82. L'article 38 prévoit une dérogation à l'obligation à de formaliser par voie de protocole les transferts de données à caractère personnel tant dans le chef des autorités qui communiqueront des données à l'autorité de certification de cybersécurité et aux autorités visées à l'article 5, §2 de l'avant-projet de loi que dans le chef de ces dernières.

83. L'Autorité rappelle que l'obligation de formaliser un échange de données visée à l'article 20 de la LTD ne s'applique pas à un échange ponctuel de données[20] ; ce qui serait le cas en cas d'application de l'article 29 du CiCr (autorités judiciaires).

[19] Ibidem

[20] Recommandation 02/2020 du 31 janvier 2020 de l'Autorité relative à la portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral, p.16.

84. Pour pourvoir déroger à cet article 20 de la LTD, la norme doit encadrer le flux structurel de données à caractère personnel visé et ce, de façon prévisible et conforme aux principes de nécessité et de proportionnalité ; ce qui nécessite de « *prévoir explicitement qui (destinataire(s)) se voit transmettre quoi (catégories des données communiquées), quand et pourquoi (finalités et modalités de la communication)* »[21] dans le respect des principes de nécessité et de proportionnalité ; ce qui doit être fait au niveau des dispositions de l'avant-projet de loi qui encadrent ces communications de données par l'Autorité nationale de certification de cybersécurité. Il est à ce sujet renvoyé aux observations précitées de l'Autorité relatives aux articles 16 et 17 de l'avant-projet de loi qui encadrent lesdites communications structurelles de données.

85. Quant aux collectes structurelles de données à caractère personnel que l'Autorité nationale de certification de cybersécurité et les autorités visées à l'article 5, §2 réaliseraient auprès des autorités sectorielles (cf. supra) pour l'exercice des missions de service public prévues par le Règlement cybersécurité, elles doivent répondre aux mêmes critères de prévisibilité pour que ces autorités sectorielles soient dispensées de les formaliser par un protocole au sens de l'article 20 de la LTD. A défaut d'être prévues par les normes qui encadrent ces autorités sectorielles (ce qu'il appartient à l'auteur de l'avant-projet de loi de vérifier), les modalités précitées desdites communications doivent être prévues par le présent avant-projet de loi pour autant qu'elles portent sur des données à caractère personnel.

Par ces motifs,

L'Autorité

Considère que l'avant-projet de loi soumis pour avis doit être adaptée en ce sens :

1. Révision des articles 6 §1 et 3, 7, 16 §2 et 3, 17 §1 et 3, 36, §1 et 3, 4° et 38 qui prévoient les échanges de données afin de les circonscrire adéquatement au strict nécessaire et proportionné au regard des objectifs du Règlement cybersécurité ou de missions de services publics connexes touchant directement à la cybersécurité conformément aux considérations générales de l'avis et aux considérations particulières relatives à ces dispositions en projet (cons. 6 à 14 et 19, 20, 37, 40, 43 , 55, 85) ;

2. Imposition d'une obligation d'information spécifique à l'Autorité nationale de certification conformément au considérant 15 ;

[21] Ibidem, p.15

3. Suppression de la mission de délivrance des certificats du champ d'application de la dérogation au devoir de confidentialité et au secret professionnel (cons. 23) ;

4. Encadrement des dérogations au devoir de confidentialité, nécessaires à la réalisation des missions d'inspection l'autorité nationale de certification et des autorités visées à l'article 5, §2, conformément au considérant 26 ;

5. Mise en place de garanties adéquates pour les éventuelles collectes de données, nécessaires à l'exercice de ces missions d'inspection, couvertes par le secret professionnel conformément au considérant 27 ;

6. Précision de l'article 13, §2 relatif à la collecte d'informations du service d'inspection conformément au considérant 31 ;

7. Ajout de garanties pour la préservation des droits et libertés des clients (personnes physiques) des prestataires ICT contrôlés (ou les personnes physiques clientes de ces clients) au regard des collectes et communications légitimes du service d'inspection (cons. 33, 38, 67) ;

8. Imposition du respect du principe de proportionnalité dans l'exercice des missions d'inspection (cons. 34) ;

9. Motivation du caractère nécessaire de la dérogation au principe de confidentialité des communications électroniques et limitation aux hypothèses strictement nécessaires, encadrement de cette dérogation conformément aux considérants 49 et 50 (cons. 45 à 50)

10. Suppression de la description des catégories de traitements de données à caractère personnel (cons. 53 et 54) ;

11. Rectification de la description des finalités des traitements de données de l'autorité nationale de certification de cybersécurité et des autorités visées à l'article 5, §2 en projet conformément au considérant 55;

12. Précision de la qualification du responsable du traitement conformément aux considérants 56 et 57.

13. Suppression des articles 36, §2 en projet (cons. 58 à 64) ;

14. Précision exhaustive des catégories de données que l'Autorité nationale de certification de cybersécurité et les autorités désignées conformément à l'article 5, §2 traiteront dans l'exercice des missions que l'avant-projet de loi leur confie conformément aux considérants 61 et s. ;

15. Adaptation des catégories de personnes concernées à propos desquelles les autorités visées à l'article 5 traiteront des données conformément aux considérants 66 et 67 ;

16. Précision de l'article 39 en projet relatif à la durée de conservation des données conformément au considérant 69 ;

17. Limitation des droits des personnes concernées consacrés par le RGPD auxquels il est dérogé aux seuls droits dont l'exercice met en péril les missions d'inspection et encadrement adéquat de ces dérogations à ces droits et à l'obligation de protocole d'échange de données prévu à l'article 20 de la LTD conformément aux considérants 73 à 81.

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 08/2022 van 21 januari 2022

Betreft: Voorontwerp van wet inzake de certificering van cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (CO-A-2021-256)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig: De heren Yves-Alexandre de Montjoye, Bart Preneel en Frank Robben;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, en met name de artikelen 23 en 26 (hierna 'WOG');

Gelet op verordening (EU) nr. 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* (hierna 'AVG');

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna de 'WVP');

Gelet op de op 30 november 2021 ontvangen adviesaanvraag van de premier, Alexander De Croo;

Gelet op de aanvullende inlichtingen die op 14 december 2021 werden ontvangen;

Brengt het volgende advies uit op 21 januari 2022:

I. Onderwerp en achtergrond van het verzoek

1. Op 30 november 2021 heeft de premier de Autoriteit om advies gevraagd over het voorontwerp van wet inzake de certificering van cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (hierna 'het voorontwerp van wet').

2. Dit voorontwerp van wet strekt tot uitvoering van verordening (EU) 2019/881 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (ICT) (hierna de 'Cyberbeveiligingsverordening').

3. Deze Cyberbeveiligingsverordening heeft tot doel het vertrouwen in de ICT-sector te vergroten door een Europees kader voor cyberbeveiligingscertificering vast te stellen, waarin horizontale voorschriften worden vastgesteld voor de ontwikkeling van certificeringsregelingen op het vlak van cyberbeveiliging voor verschillende categorieën ICT-producten[1], -diensten[2] en -processen[3]. ENISA is verantwoordelijk voor het opstellen van certificeringsregelingen, die vervolgens door de Europese Commissie zullen worden aangenomen door middel van uitvoeringshandelingen. Een Europese cyberbeveiligingscertificeringsregeling is volgens de Cyberbeveiligingsverordening *"een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale overheidsinstantie zijn ontwikkeld en vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-producten, -diensten en -processen die onder het toepassingsgebied van de specifieke regeling vallen".* In elke certificeringsregeling wordt onder meer gespecificeerd op welke soort of categorieën ICT-producten, -diensten en -processen ze betrekking heeft, wat het doel is, welke normen er gelden en welke evaluatiemethoden er worden gebruikt. De Europese cyberbeveiligingscertificaten, afgegeven door de conformiteitsbeoordelingsinstanties die door nationale accreditatie-instanties zijn geaccrediteerd, bevestigen dat een ICT-product, -dienst of -proces is beoordeeld op het vlak van de naleving van de specifieke beveiligingseisen die in een Europese cyberbeveiligingscertificeringsregeling zijn vastgesteld. De Cyberbeveiligingsverordening definieert drie zekerheidsniveaus, die in verhouding staan tot verschillende risiconiveaus. Het gaat om de volgende niveaus: basis, substantieel en hoog.

---

[1] In de Cyberbeveiligingsverordening gedefinieerd als *"een element of groep elementen van een netwerk- of informatiesysteem".*

[2] In de Cyberbeveiligingsverordening gedefinieerd als *"een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen".*

[3] In de Cyberbeveiligingsverordening gedefinieerd als *"een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren ofonderhouden".*

4. Tenzij in het recht van de Europese Unie of in de nationale wetgeving van een lidstaat anders is bepaald, vindt de certificering of de conformiteitsverklaring op vrijwillige basis plaats. De Europese Commissie zal op geregelde tijdstippen nagaan of het nodig is om certificaten verplicht te stellen. De Cyberbeveiligingsverordening voorziet in de mogelijkheid om zich te laten certificeren of over te gaan tot een conformiteitsverklaring. Een certificaat wordt afgegeven door een onafhankelijke en geaccrediteerde conformiteitsbeoordelingsinstantie. Een conformiteitsverklaring wordt afgegeven onder de verantwoordelijkheid van de ICT-fabrikant of -leverancier door middel van een zelfbeoordeling. In elke certificeringsregeling wordt aangegeven of een dergelijke conformiteitsverklaring al dan niet is toegestaan en de zelfbeoordeling is beperkt tot het 'basis'-zekerheidsniveau.

5. De lidstaten moeten, ter uitvoering van deze verordening, de nationale cyberbeveiligingscertificeringsautoriteit of -autoriteiten aanwijzen, die certificaten zullen afgeven, of zullen instaan voor het toezicht en de controle op de correcte toepassing van de regels door de verschillende actoren (fabrikanten, leveranciers en aanbieders van ICT-producten en -diensten die houder zijn van een certificaat of die een conformiteitsverklaring hebben afgegeven, en conformiteitsbeoordelingsinstanties). Bovendien moeten de lidstaten in hun nationale wetgeving specifieke regels vaststellen om de correcte toepassing van deze verordening te waarborgen, bijvoorbeeld met betrekking tot sancties of de intrekking van certificaten. Dat is het onderwerp van het voorontwerp van wet dat voor advies is voorgelegd.

II. Onderzoek

Algemene opmerkingen – Mededeling van gegevens door de autoriteiten die belast zijn met de controle op de naleving van de Cyberbeveiligingsverordening en de Europese regelingen voor de cyberbeveiligingscertificering en de bescherming van de klanten (natuurlijke personen) van de gecontroleerde aanbieders van ICT-diensten (of van de klanten-natuurlijke personen van dergelijke klanten van wie de gegevens zijn opgenomen in de gecontroleerde ICT-diensten)

6. Dit advies van de Autoriteit is slechts geldig voor zover gegevensverwerkingen met betrekking tot natuurlijke personen onder de bepalingen van het voorontwerp van wet vallen. De gegevensverwerkingen die moeten worden uitgevoerd in het kader van de door de Cyberbeveiligingsverordening vereiste controles, kunnen betrekking hebben op persoonsgegevens in de zin van de AVG wanneer de fabrikanten of leveranciers van ICT-producten, de aanbieders van ICT-diensten of van ICT-processen die houder of aanvrager zijn van een Europees conformiteitscertificaat inzake cyberbeveiliging, natuurlijke personen zijn, maar ook wanneer de controle van de naleving van de certificeringsregelingen door de leveranciers van deze

gecertificeerde ICT-diensten de verwerking van persoonsgegevens met zich meebrengt, zoals de gegevens van hun klanten-natuurlijke personen of de klanten-natuurlijke personen van hun klanten. Laten we de clouddiensten[4] als voorbeeld nemen: het is gebruikelijk dat de klanten van een aanbieder van clouddiensten deze diensten gebruiken voor hun eigen verwerkingen van persoonsgegevens, waarbij het kan gaan om bijzondere categorieën van gegevens in de zin van de AVG, afhankelijk van het werkterrein van die klanten (bv. een ziekenhuis, een advocatenkantoor of een overheidsinstantie die belast is met de preventie en opsporing van strafrechtelijke inbreuken).

7. Zoals de European Data Protection Supervisor heeft opgemerkt in een van zijn recente adviezen over de Europese strategie voor cyberbeveiliging en over de richtlijn NIS 2.1[5]: *"Article 5(1)(f) of Regulation (EU) 2016/679 (GDPR) has established security as one of the main principles relating to the processing of personal data. Article 32 GDPR further defines this obligation, applicable to both controllers and processors, to ensure an appropriate level of security. Both provisions make clear that security is essential for compliance with EU data protection law. This is why (...) improving cybersecurity is essential for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data (...). At the same time (...) the pursuance of the objectives of cybersecurity may lead to deploying measures that interfere with the rights to data protection and privacy of individuals. This means ensuring that any potential limitation of the right to the protection of personal data and privacy must fulfil the requirements of Article 52(1) of EU Charter of Fundamental Rights, in particular being achieved by way of a legislative measure, being both necessary and proportionate, and respecting the essence of the right."*

8. In het licht van deze overwegingen is het voorontwerp van wet problematisch omdat het voorziet in zeer ruime gegevensuitwisselingen tussen enerzijds de nationale cyberbeveiligingscertificeringsautoriteit en de andere autoriteiten die zullen worden aangewezen voor de uitvoering van de in de Cyberbeveiligingsverordening bedoelde controle-opdrachten, en anderzijds de volgende autoriteiten: de gerechtelijke overheden, de sectorale overheden of de inspectiediensten respectievelijk bedoeld 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, de markttoezichtautoriteiten, de nationale

---

[4] Cf. EUCS, a candidate cybersecurity certification scheme for cloud services, december 2020, beschikbaar op de ENISA-website: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@@download/fullReport. Er wordt bepaald dat "the EUCS scheme may cover any type of ICT service, provided that the ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface (ISO 17788) and that the ICT service aims at reaching the assurance level corresponding to one of the three levels "basic", "substantial" and "high" of the EUCSA as defined in the EUCS scheme".

[5] EDPS Opinion 05/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, beschikbaar op de website van de EDPS op https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en.

accreditatieautoriteit, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid.

9. Deze uitwisselingen doen vragen rijzen in verband met hun zeer ruime onderwerp, zoals thans in het voorontwerp van wet is bepaald. Meermaals wordt namelijk bepaald dat zij niet alleen plaatsvinden voor de uitoefening van openbaredienstopdrachten die bestaan in de controle op de naleving van de Cyberbeveiligingsverordening en de Europese cyberbeveiligingscertificeringsregelingen of de conformiteitsverklaringen die ter uitvoering van de genoemde verordening worden afgegeven, maar ook voor de toepassing van andere wettelijke bepalingen (zonder te specificeren om welke wettelijke bepaling het gaat; op die manier kan niet worden nagegaan of er een duidelijk verband bestaat met de bovengenoemde Cyberbeveiligingsverordening). Dit lijkt onevenredig, niet conform het toepassingsgebied van het voorontwerp van wet dat de Cyberbeveiligingsverordening ten uitvoer moet leggen, volgens de algemene overwegingen van de memorie van toelichting.

10. Bovendien dreigt dit gebrek aan een minimumkader voor dergelijke uitwisselingen de door de Europese cyberbeveiligingsverordening nagestreefde doelstelling van vertrouwen in gecertificeerde ICT-producten en -diensten te ondermijnen, aangezien de gegevens van de klanten (of hun klanten) van door de cyberbeveiligingscertificeringsautoriteit gecontroleerde ICT-dienstverleners volgens de formulering van het wetsontwerp kunnen worden verzameld en gebruikt door overheidsdiensten die geen specifieke cyberbeveiligingsopdracht hebben, zoals politie of inlichtingendiensten, voor hun eigen opdrachten van preventie en opsporing van strafbare feiten, onderzoek en vervolging, of zelfs voor opdrachten van de Staatsveiligheid en de Algemene Inlichtingen- en Veiligheidsdienst. Deze situatie kan een belemmering vormen voor de bevordering van ICT-diensten en -producten die gecertificeerd zijn in overeenstemming met de Cyberbeveiligingsverordening, en bijgevolg voor de verbetering van de informatiebeveiliging op deze gebieden.

11. De auteur van het voorontwerp van wet moet daarom de uitwisselingen regelen in overeenstemming met wat strikt noodzakelijk en redelijk is in het licht van het toepassingsgebied en de doelstellingen van de Cyberbeveiligingsverordening. In artikel 58.7.a van de Cyberbeveiligingsverordening wordt trouwens bepaald dat de nationale cyberbeveiligingscertificeringsautoriteiten uitsluitend in samenwerking met *"andere betrokken markttoezichtautoriteiten* " moeten toezien op de naleving van de in de Europese cyberbeveiligingscertificeringsregelingen opgenomen regels en die regels moeten handhaven, en niet om het even welke overheidsinstantie. Artikel 58.7.h van die verordening bepaalt dan weer

het volgende: nationale cyberbeveiligingscertificeringsautoriteiten *"werken samen met andere nationale cyberbeveiligingscertificeringautoriteiten of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-conformiteit van ICT-producten, -diensten en -processen met de voorschriften van deze verordening of met de voorschriften van specifieke Europese cyberbeveiligingscertificeringsregelingen"*. In overweging 102 van deze verordening wordt in dat verband het volgende gespecificeerd: *"De Commissie moet die informatie-uitwisseling bevorderen door een algemeen elektronisch informatieondersteuningssysteem beschikbaar te stellen, bijvoorbeeld het informatie- en communicatiesysteem voor markttoezicht (ICSMS) en het systeem voor snelle waarschuwingen over gevaarlijke niet-levensmiddelen (Rapex), die overeenkomstig Verordening (EG) nr. 765/2008 al door markttoezichtautoriteiten worden gebruikt."* Dit voorbeeld van het melden van waarschuwingen over de aanwezigheid van producten of diensten die niet voldoen aan een certificeringsregeling, sluit goed aan bij het Europees kader voor cyberbeveiligingscertificering, zoals beschreven in artikel 46 van de Cyberbeveiligingsverordening. De Autoriteit is bijgevolg van oordeel dat de bedoelde uitwisselingen beperkt moeten blijven tot de verwezenlijking van deze doelstelling en geen ruimte mogen laten voor de toepassing van om het even welke wettelijke bepaling. Dit delen van informatie over de niet-naleving, door ICT-producten, -diensten en -processen, van de vereisten van de Cyberbeveiligingsverordening of van bepaalde specifieke Europese cyberbeveiligingscertificeringsregelingen vereist volgens de Autoriteit geen uitwisseling van de persoonsgegevens die de genoemde klanten in het kader van hun contractuele relatie aan de genoemde dienstverleners ter beschikking stellen.

12. Op de vraag wat de gegevensuitwisseling met de verschillende in artikel 6, § 3, van het voorontwerp bedoelde autoriteiten rechtvaardigt, antwoordde de afgevaardigde van de minister het volgende:
    a. Met betrekking tot de gerechtelijke autoriteiten: *"Il apparaît nécessaire que les autorités judiciaires puissent solliciter ou être notifiées des informations en cas d'infractions pénales (fraudes liées à la délivrance, aux contrôles, aux sanctions et aux réclamations des certifications de cybersécurité ou d'infractions pénales prévues par les différentes législations sectorielles - dont la loi NIS."* In dit verband merkt de Autoriteit in de eerste plaats op dat bij lezing van het voorontwerp van wet inbreuken op de Cyberbeveiligingsverordening en de Europese certificeringsregelingen enkel worden bestraft via de wijziging van het Wetboek van Economisch Recht en dat boek XV van dit wetboek reeds de gegevensmededeling regelt die de economische inspectie bij de uitoefening van haar opdrachten kan verrichten. Vervolgens wordt in artikel 29 van het Wetboek van Strafvordering (Sv.) reeds het volgende bepaald: *"Iedere gestelde overheid, ieder openbaar officier of ambtenaar (...) die in de uitoefening van zijn ambt kennis krijgt van een misdaad of van een wanbedrijf, is verplicht daarvan dadelijk bericht te geven aan*

de procureur des Konings bij de rechtbank binnen wier rechtsgebied die misdaad of dat wanbedrijf is gepleegd of de verdachte zou kunnen worden gevonden, en aan die magistraat alle desbetreffende inlichtingen, processen-verbaal en akten te doen toekomen." Het is niet nodig, en vanuit het oogpunt van de bescherming van persoonsgegevens zelfs contraproductief, om deze mededeling van gegevens in het voorontwerp van wet te herhalen zonder de modaliteiten ervan vast te leggen, temeer daar in artikel 29 Sv. de inachtneming van bepaalde formaliteiten in dit verband wordt opgelegd. De Autoriteit beveelt bijgevolg aan deze uitwisseling uit het voorontwerp van wet te schrappen.

b. Met betrekking tot de sectorale autoriteiten (NIS)[6]: *"Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle des mesures de sécurité des réseaux et systèmes d'informations (P.S.I., voir article 21 et suivants de la loi NIS), qui serait titulaire*

[6] Zoals uit de aanvullende informatie blijkt, gaat het om de volgende autoriteiten:

"Les autorités sectorielles visées à l'article 3, § 3 de l'avant-projet de loi sont les autorités 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 (ci-après, "loi NIS").

Il s'agit concrètement des autorités suivantes :

- *Désignées par la loi NIS :*
  - *La BNB (art. 95. de la loi NIS qui a inséré un article 36/47 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique).*
  - *La FSMA (art. 90 et 91 de la loi NIS ayant modifiés les art. 71 et 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers).*
  - *L'IBPT (art. 88. de la loi NIS qui a modifié l'art. 14, § 1er, alinéa 1er, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges).*
- *Désignées par l'annexe 1 de l'arrêté royal du 12 juillet 2019 (portant exécution 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, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques) :*
  - *pour le secteur de l'énergie : le Ministre fédéral ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des transports :*
    - *En ce qui concerne le secteur du transport, à l'exception du transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour le Transport, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
    - *En ce qui concerne le transport par voies d'eau accessibles aux navires maritimes : le Ministre fédéral compétent pour la Mobilité maritime, ou par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur de la santé : le Ministre fédéral ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
  - *pour le secteur des fournisseurs de service numérique : le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration (le cas échéant, le Ministre peut désigner un délégué différent par sous-secteur).*
- *Désignée par l'arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable :*
  - *le Comité national de sécurité pour la fourniture et la distribution d'eau potable."*

ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant."

In dit verband begrijpt de Autoriteit dat deze sectorale autoriteiten, die specifieke opdrachten hebben op het gebied van informatiebeveiliging, ervan in kennis moeten worden gesteld dat de organisaties waarvan zij de naleving van de bepalingen van de bovengenoemde wet van 7 april 2019 (bekend als de NIS-wet) controleren, gebruikmaken van gecertificeerde ICT-diensten of -producten waarvan de niet-naleving van de certificeringsregeling is vastgesteld door de nationale certificeringsautoriteit of door een autoriteit die is aangewezen ter uitvoering van artikel 5, § 2 van het voorontwerp van wet. In dit verband vraagt de Autoriteit zich af of de maatregelen tot intrekking van een certificering – die door hun aard aan publiciteitsmaatregelen zouden moeten worden onderworpen – hiervoor niet zouden moeten volstaan. Indien dit niet het geval zou zijn (wat in de memorie van toelichting zou moeten worden gemotiveerd), is de Autoriteit, gezien de met de cyberbeveiliging verband houdende aard van de opdrachten van de krachtens de NIS-wet opgerichte controle-autoriteiten, van oordeel dat deze uitwisselingen noodzakelijk lijken, maar dat het, naast het geven van een definitie van het in het voorontwerp van wet gebruikte begrip *"sectorale autoriteiten"* (uitdrukkelijke vermelding van de bedoelde autoriteiten), noodzakelijk is om in het voorontwerp van wet[7] duidelijk de omstandigheden en modaliteiten te bepalen van deze gegevensmededelingen door de nationale cyberbeveiligingscertificeringsautoriteit en de krachtens artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten, alsook het doel van de verwerking die door de bedoelde sectorale autoriteiten met deze informatie zal worden verricht. Bovendien moet dan ook worden voorzien in de beperking van de uitwisselingen over de vaststelling van een inbreuk op de informatiebeveiligingsnormen waarop deze autoriteiten controle uitoefenen, tot louter de entiteiten die onder het toezicht van de genoemde autoriteiten staan,

c. Met betrekking tot de markttoezichtautoriteiten: *"Ces autorités ont besoin de savoir, dans le cadre de leurs missions de contrôle portant sur les mesures de sécurité appliquées par les entités sur lesquelles elles ont une compétence de contrôle, qui serait titulaire ou non d'un certificat européen de cybersécurité et ne serait pas en conformité avec le schéma de certification correspondant."*

Indien deze markttoezichtautoriteiten specifieke opdrachten hebben op het gebied van cyberbeveiliging, die de auteur van het voorontwerp van wet moet motiveren, en indien

[7] voor zover deze bijzonderheden niet reeds in de NIS-wet zijn opgenomen, wat de auteur van het voorontwerp van wet moet nagaan.

niet reeds elders is voorzien in dergelijke mededelingen betreffende de certificering van de betrokken entiteiten, lijken de bedoelde mededelingen relevant en noodzakelijk, maar voor de passende regeling ervan wordt verwezen naar de eerdere opmerkingen betreffende de sectorale autoriteiten (aanduiding van de toezichtautoriteiten die als enige over een dergelijke bevoegdheid beschikken, beperking van de uitwisselingen betreffende de vaststelling van een inbreuk op de informatiebeveiligingsnormen waarop deze markttoezichtautoriteiten controle uitoefenen tot louter de entiteiten die onder het toezicht van de genoemde autoriteiten staan, enz.). Zo niet, dan moet deze mededeling uit het voorontwerp van wet worden geschrapt.

d. Met betrekking tot de openbare veiligheidsdiensten: *"Dans le cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou dans le cas où ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services."*

Op de vraag welke autoriteiten onder dit begrip *"openbare veiligheidsdiensten"* vallen, preciseerde de afgevaardigde van de minister dat het om de volgende autoriteiten gaat: *"SPF Intérieur, Bruxelles Prévention et Sécurité, Service public de Wallonie, Vlaamse Overheid, Administrations publiques locales (provinces et communes), Gouverneurs, OCAM."*

Naast van het ontbreken van een definitie in het voorontwerp van wet van het begrip 'openbare veiligheidsdienst' (wat zou moeten worden rechtgezet door een uitdrukkelijke vermelding van de genoemde autoriteiten of eerder, in de meeste gevallen, van hun dienst die belast is met de openbare veiligheid), maakt het ontbreken van een minimumkader voor deze uitwisselingen deze onvoorspelbaar. Zoals uit de aanvullende informatie blijkt, moeten die worden beperkt tot de gevallen waarin een verplichte certificering door die autoriteiten is opgelegd om redenen van openbare veiligheid, en moet worden bepaald dat de maatregelen tot intrekking of schorsing van het certificaat van een entiteit (die aan deze verplichte certificering is onderworpen) alleen worden meegedeeld aan de autoriteit die is aangeduid in de norm die deze verplichte certificering oplegt. Dit is alleen het geval als er geen publiciteitsmaatregelen zijn voor de intrekking van een dergelijk certificaat wegens niet-naleving van de certificeringsregeling, wat in de memorie van toelichting moet worden gemotiveerd.

e. Wat de inlichtingendiensten betreft*: "Ils ont pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux menaces graves contre la sûreté de l'Etat. Lorsque cela s'avérerait nécessaire dans leurs recherches, par exemple lorsqu'une entité titulaire d'un certificat européen de cybersécurité aurait des liens avec des activités d'espionnage ou liées à une organisation criminelle, les services de renseignements devraient pouvoir avoir accès (en vertu de l'art. 14, al. 2 et art. 20, § 1er de la loi du 30 novembre 1998 sur les services de renseignement) aux informations collectées par le service d'inspection de l'autorité nationale de certification dans le cadre de ses missions de contrôle, au regard de l'importance de l'intérêt général protégé. En outre, dans la cas où ces autorités utiliseraient des équipements ou des services faisant l'objet d'une certification européenne de cybersécurité ou ces autorités imposeraient, dans le cadre de leurs missions de sécurité publique, à d'autres entités l'obtention d'un certificat européen de cybersécurité, elles doivent pouvoir prévenir l'autorité chargée des missions des chapitres 5 et 6 de toute non-conformité par rapport au schéma qu'elles auraient constatées ou être prévenues, lorsque cela menace la bonne exécution de leurs services. Faut encore qu'elles disposent de pouvoir d'investigation à ce sujet."*

In dit verband is de Autoriteit, naast de bovenstaande overwegingen met betrekking tot de publiciteitsmaatregelen voor de intrekking en schorsing van certificaten en naar het voorbeeld van de opmerking met betrekking tot de gerechtelijke autoriteiten, van mening dat het niet nodig is, of zelfs contraproductief vanuit het oogpunt van de bescherming van persoonsgegevens, om een mededeling van gegevens aan de inlichtingendiensten, die reeds in hun eigen organieke wetgeving is geregeld, te herhalen. Bovendien valt dit buiten het toepassingsgebied van dit voorontwerp van wet. Daarom moet deze uitwisseling ook worden geschrapt.

f. Met betrekking tot de politie: *"pour les mêmes motifs que ceux prévus pour les services de sécurité publique et les autorités judiciaires"*.

De Autoriteit verwijst naar haar bovengenoemde opmerkingen over dit onderwerp.

13. Bijgevolg dient de formulering van de bepalingen van het voorontwerp die voorzien in deze uitwisselingen (artt. 6, §§ 1 en 3, 7, 16, § 2, 17, §§ 1 en 3, 36, §§ 1 en 3, 4° en 38) te worden herzien om ze in overeenstemming te brengen met de bovenstaande overwegingen door ze te beperken tot wat vereist is voor de verwezenlijking van de doelstellingen van de Cyberbeveiligingsverordening of opdrachten van verwante openbare diensten die rechtstreeks betrekking hebben op de cyberbeveiliging, zoals de opdrachten die worden uitgeoefend door de toezichthoudende autoriteiten zoals bedoeld in de NIS-wet (sectorale autoriteiten). De auteur van

het voorontwerp van wet moet erover waken niet te voorzien in mededelingen van persoonsgegevens waarin reeds is voorzien door andere wettelijke bepalingen.

14. Teneinde de rechten en vrijheden te vrijwaren van de natuurlijke personen, die klant zijn van de onder toezicht staande dienstverleners en die de gevolgen kunnen ondervinden van deze uitwisselingen, is het bovendien absoluut noodzakelijk om in het wetsontwerp een bepaling op te nemen die stelt dat deze uitwisselingen geen betrekking mogen hebben op persoonsgegevens van klanten-natuurlijke personen (of klanten-natuurlijke personen van die laatsten) van de onder toezicht staande ICT-dienstverleners, gelet op de aanzienlijke risico's die dit inhoudt voor deze betrokkenen en gelet op het feit dat uit de door de afgevaardigde van de minister aangevoerde rechtvaardigingsgronden niet blijkt dat deze informatie in dit geval relevant en noodzakelijk is.

15. Tot slot is het, gelet op de doelstellingen van de Europese Cyberbeveiligingsverordening, van belang dat in het voorontwerp van wet expliciet een informatieplicht inzake de uitgevoerde intrekkingen van certificaten wordt opgelegd aan de nationale cyberbeveiligingscertificeringsautoriteit die belast zal zijn met de intrekking van de certificaten. Daartoe moet deze autoriteit worden verplicht om te beschikken over een openbare website en een informatiedienst (push) die alle betrokken actoren op de hoogte brengt van elke certificeringsintrekking. Dit vereist geen openbaarmaking van persoonsgegevens en is in overeenstemming met een van de doelstellingen van de Europese Cyberbeveiligingsverordening, namelijk het vertrouwen in gecertificeerde ICT-producten, -diensten en -processen te waarborgen. In voorkomend geval zou een uitzondering op deze openbaarmaking kunnen worden overwogen voor ICT-producten of -diensten die voor hun gebruik een veiligheidsmachtiging vereisen. In het algemeen moet elke uitzondering op de openbaarmaking van informatie over de herroeping of afgifte van certificaten uitdrukkelijk in het voorontwerp van wet worden opgenomen en naar behoren worden gemotiveerd en verantwoord in de memorie van toelichting.

Bijzondere opmerkingen

Toepassingsgebied van het wetsontwerp

16. Artikel 3 van het wetsontwerp bepaalt het toepassingsgebied ervan door te specificeren dat het wetsontwerp van toepassing zal zijn op vrijwillige Europese certificering van de cyberbeveiliging van ICT-producten, -diensten en -processen zoals bedoeld in de Cyberbeveiligingsverordening en dat alleen de hoofdstukken 1 tot 4 en 7 en de artikelen 21 en 22 van dit wetsontwerp ook van toepassing zijn op de verplichte certificeringen.

17. Uit de aanvullende inlichtingen blijkt het volgende: *"Les mesures de contrôle et de sanctions liées aux certifications rendues obligatoires sont réglées ou devront être réglées par les différentes législations sectorielles applicables."* Op de vraag waarom hoofdstuk 8, dat handelt over de verwerking van persoonsgegevens ter uitvoering van het wetsontwerp, was uitgesloten van de verplichte Europese cyberbeveiligingscertificeringen, antwoordde de afgevaardigde van de minister dat dit een vergetelheid was en dat hoofdstuk 8 kon worden opgenomen in artikel 3, § 2 van het wetsontwerp. Hiervan is nota genomen.

Aanwijzing van de bevoegde toezichthoudende autoriteiten

18. Ter uitvoering van artikel 58 van de Cyberbeveiligingsverordening delegeert artikel 5 van het wetsontwerp aan de Koning de taak om de nationale cyberbeveiligingscertificeringsautoriteit aan te wijzen die zal worden belast met de controle- en toezichthoudende taken, bedoeld in artikel 58 van deze verordening. In de tweede paragraaf van deze bepaling wordt bepaald dat de Koning, *"naargelang het voorwerp van de betrokken certificeringsregeling en op verzoek van de betrokken overheid "*, de controle- en sanctietaken (met uitzondering van de intrekking en schorsing van certificaten) aan een andere overheid kan toevertrouwen. Hierover ondervraagd, specificeerde de afgevaardigde van de minister als volgt: *"Concrètement, il est envisagé d'utiliser éventuellement ce mécanisme au profit de l'IBPT, la FSMA, la BNB et l'inspection économique. Les dispositions modificatives ont été insérées dans le projet de loi à la demande de ces autorités car ces dernières considéraient les dispositions modificatives comme nécessaires pour que le Roi puisse éventuellement, dans les conditions imposées par la loi, les désigner."*[8] Hiervan is nota genomen.

Samenwerking op nationaal niveau (art. 6)

19. Artikel 6 van het voorontwerp van wet heeft betrekking op de samenwerking en gegevensuitwisseling op nationaal niveau die de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die zullen worden aangewezen ter uitvoering van artikel 5, § 2 van het ontwerp (voor de uitvoering van de opdrachten bedoeld in de hoofdstukken 5 en 6 van het voorontwerp van wet) alsook andere overheidsautoriteiten zullen uitvoeren voor de toepassing van de Cyberbeveiligingsverordening en elke andere wettelijke bepaling.

20. In dit verband wordt verwezen naar het commentaar in de algemene opmerkingen van dit advies.

[8] Gezien de aanwijzingen die reeds via de wijzigingsbepalingen zijn gedaan, vraagt de Autoriteit zich af of het artikel 5, § 2 van het ontwerp wel nodig is. Het verdient aanbeveling dat de auteur van het voorontwerp van wet dit in zijn voorontwerp verduidelijkt. In het vervolg van het ontwerpadvies zullen deze autoriteiten zonder onderscheid worden aangeduid als "ter uitvoering van artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten".

21. Indien de nationale cyberbeveiligingscertificeringsautoriteit en de in artikel 5, § 2 bedoelde autoriteiten structureel persoonsgegevens moeten verzamelen bij deze sectorale autoriteiten voor de uitoefening van de in de Cyberbeveiligingsverordening bedoelde openbaredienstopdrachten, moeten deze gegevensverzamelingen ook in het voorontwerp van wet worden opgenomen en aan dezelfde criteria inzake voorzienbaarheid voldoen; dit lijkt momenteel niet het geval te zijn.

22. Wat artikel 6, § 2, van het ontwerp betreft, dat houders van Europese cyberbeveiligingscertificaten en afgevers van conformiteitsverklaringen verplicht om de autoriteiten die belast zijn met het toezicht op de naleving van de Cyberbeveiligingsverordening en de Europese certificeringsregelingen alle informatie te verstrekken die zij nodig hebben voor de uitvoering van hun taken, lijkt deze ontwerpbepaling overtollig te zijn met de bepalingen van het voorontwerp die de inspectiebevoegdheden van de inspectiediensten van deze autoriteiten regelen en moet ze bijgevolg uit dit deel van het voorontwerp van wet te worden geschrapt.

Uitwisseling van gegevens die beschermd zijn door het beroepsgeheim of door een geheimhoudingsplicht (art. 6, § 4)

23. Artikel 6, § 4 van het ontwerp heeft betrekking op de kwestie van door het beroepsgeheim beschermde gegevens die zich zal voordoen in het kader van de uitwisseling van gegevens die de nationale cyberbeveilingscertificeringsautoriteit en de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten zullen hebben met derden, in deze bewoordingen:

"§ 4. Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen of vertrouwelijke informatie die hun zijn toevertrouwd, mogen deze geheimen of vertrouwelijke informatie bekendmaken aan de autoriteit bedoeld in artikel 5, § 1, alsook eventueel aan andere overheden indien dit nodig is voor de toepassing van de Cyberbeveiligingsverordening of deze wet.

Het gaat met name om noodzakelijke informatie met betrekking tot de afgifte van certificaten, het toezicht, sancties en klachten. Indien deze informatie persoonsgegevens betreft, is hoofdstuk 8 van toepassing. De regelingen voor de uitwisseling van informatie dienen het vertrouwelijke karakter van de betrokken informatie te eerbiedigen."

24. Ten eerste ziet de Autoriteit niet in hoe voor de afgifte van beveiligingscertificaten informatie moet worden verzameld die onder het beroepsgeheim of onder een geheimhoudingsplicht valt. Volgens de memorie van toelichting wordt alleen de controle-opdracht genoemd als opdracht met mogelijke gevolgen voor het beroepsgeheim. Uit de aanvullende inlichtingen die zijn verkregen van de afgevaardigde van de minister, komt geen enkele rechtvaardiging naar voren voor de impact van de opdracht inzake de afgifte van beveiligingscertificaten op het beroepsgeheim. Bij gebrek aan een afdoende rechtvaardiging in de memorie van toelichting moeten de woorden *"afgifte van certificaten"* bijgevolg uit artikel 6, § 4, tweede lid, worden weggelaten.

25. Vervolgens merkt de Autoriteit op dat, wat de uitwisseling van gegevens betreft die beschermd zijn door het beroepsgeheim of door een geheimhoudingsplicht, er twee gevallen moeten worden onderscheiden:
    a. in de eerste plaats de situatie van een autoriteit die aan een geheimhoudingsplicht is onderworpen en die belet wordt om onder die geheimhoudingsplicht vallende informatie mee te delen, ook al is die mededeling legitiem, relevant en noodzakelijk (cf. supra);
    b. ten tweede, het verzamelen, door de inspectiediensten van de autoriteiten die belast zijn met de controle van de naleving van de Cyberbeveiligingsverordening, van persoonsgegevens die beschermd zijn door het beroepsgeheim (bijvoorbeeld tijdens audits van gecertificeerde ICT-systemen).

26. Deze twee situaties moeten in het voorontwerp van wet afzonderlijk worden behandeld en alleen de eerste moet aan de orde komen in artikel 6, gelet op de titel ervan (*"samenwerking op nationaal niveau"*).

27. De wettelijke bepaling betreffende de eerste situatie (23.a) moet zodanig worden geformuleerd dat de opheffing van de geheimhouding alleen kan gebeuren ten behoeve van autoriteiten waarvoor de uitwisseling van gegevens legitiem[9], relevant en noodzakelijk is (cf. supra) voor de uitoefening van de inspectietaken van de autoriteiten zoals bedoeld in artikel 5 van het voorontwerp van wet. Bovendien moeten het woord/de woorden *"notamment"/"met name"* in het tweede lid van § 4 van artikel 6 van het ontwerp worden geschrapt om het voorwerp van de bedoelde uitwisselingen correct te beperken.

28. De tweede situatie van gegevensuitwisseling met gevolgen voor het beroepsgeheim moet worden behandeld in het hoofdstuk over de inspectiebevoegdheden. Het voorontwerp van wet moet noodzakelijkerwijs duidelijk voorzien in specifieke waarborgen voor de rechten en vrijheden van de personen op wie de onder het beroepsgeheim vallende gegevens betrekking hebben, indien en slechts indien de toegang tot die gegevens onontbeerlijk is voor de uitvoering van onderzoeksmaatregelen door de inspectiedienst (voorafgaande toestemming van de onderzoeksrechter, tussenkomst van de beroepsorde waartoe de persoon behoort van wie de documenten met het oog op de uitvoering van de voornoemde controles moeten worden geraadpleegd op straffe van het in het gedrang brengen van voornoemde controles, verbod op bewaring van onder het beroepsgeheim vallende documenten door voornoemde autoriteiten, ..., cf. in die zin de artikelen 56*bis* en 90*octies* van het Wetboek van Strafvordering). Zo niet, dan moet uitdrukkelijk worden bepaald dat inlichtingen die onder het beroepsgeheim vallen in de zin van artikel 458 van het Strafwetboek, niet door de inspectiedienst mogen worden verzameld.

[9] Onder verwijzing naar de bepaling in het voorontwerp van wet die de modaliteiten van deze uitwisselingen zal beschrijven in overeenstemming met de opmerkingen van de Autoriteit (cf. supra).

Hoofdstuk 5 – Toezicht (artt. 13 t/m 18)

29. De artikelen 13 tot en met 18 van het wetsontwerp voorzien in een kader voor de controleprocedure van de nationale cyberbeveiligingscertificeringsautoriteit en in de bevoegdheden die haar inspectiedienst zal hebben.

30. In artikel 13, § 2 van het voorontwerp worden de verzoeken om informatie die de inspecteurs bij de uitoefening van hun taak kunnen doen, formeel vastgelegd in de volgende bewoordingen:
"Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt."

31. Om de gecontroleerde persoon in staat te stellen de relevantie en noodzaak te beoordelen van de gegevens (in voorkomend geval persoonsgegevens) die in dit verband nodig zullen zijn, moet in deze bepaling uitdrukkelijk worden vermeld dat de inspecteurs de wettelijke bepalingen of het deel (de delen) van de certificeringsregeling waarop een inbreuk wordt vermoed, moeten identificeren.

Controlebevoegdheden van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit – Invoering van waarborgen voor de bescherming van persoonsgegevens die zijn opgenomen in de geauditeerde IT-systemen

32. De ruime controlebevoegdheden van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit worden beschreven in artikel 15 van het voorontwerp van wet.

33. Naar het voorbeeld van wat is bepaald voor de huiszoekingen artikel 15, § 4 van het ontwerp, beveelt de Autoriteit aan om in het voorontwerp van wet waarborgen toe te voegen voor bevoegdheden die bijzonder intrusief zijn en waardoor de inspectiedienst toegang krijgt tot de persoonsgegevens van de klanten (of klanten van die klanten) van de ICT-dienstverleners of van leveranciers van ICT-producten die zullen worden geïnspecteerd. Daartoe moet, als waarborg voor de bescherming van de rechten en vrijheden van de betrokkenen, aan de inspectiedienst uitdrukkelijk worden verboden de gegevens van de klanten (of van de klanten van die klanten) van de gecontroleerde dienstverleners en leveranciers te verzamelen of mee te delen voor andere doeleinden dan het toezicht op de naleving van de verordening of van de betrokken certificeringsregeling. Evenzo is de Autoriteit van oordeel dat moet worden bepaald, naar het voorbeeld van wat is vastgelegd in artikel 66 van de voornoemde wet van 7 april 2019 (NIS-wet),

dat zodra andere persoonsgegevens dan die betreffende de houder van het Europees certificaat of zijn personeelsleden moeten worden geraadpleegd met het oog op de uitvoering van controles door de inspectiedienst, deze gegevens, indien mogelijk, eerst moeten worden gepseudonimiseerd in overeenstemming met de huidige regels van de kunst.[10].

34. De Autoriteit beveelt ook aan om de naleving van het evenredigheidsbeginsel bij de uitoefening van onderzoeksbevoegdheden uitdrukkelijk in het voorontwerp van wet op te nemen, zoals dat ook het geval is voor andere inspectiebevoegdheden, zoals die van de sociale inspectie (cf. Sociaal Strafwetboek). Zo moet in artikel 15 van het voorontwerp van wet uitdrukkelijk het volgende worden bepaald: "Bij de uitoefening van hun in dit artikel bedoelde controlebevoegdheden moeten de inspecteurs van de nationale cyberbeveiligingscertificeringsautoriteit en van de autoriteiten bedoeld in artikel 5, § 2 van het ontwerp ervoor zorgen dat de middelen die zij gebruiken, geschikt en noodzakelijk zijn voor het toezicht op de Cyberbeveiligingsverordening of op de bepalingen van het certificeringsschema waarvan zij de naleving controleren." Het verzamelen van persoonsgegevens bij de uitoefening van hun toezichthoudende taken moet beperkt blijven tot uitsluitend die gegevens die relevant zijn voor het aantonen van een inbreuk op de Cyberbeveiligingsverordening of de niet-naleving van een certificeringsregeling. In dit verband beschikken zij trouwens niet over andere bevoegdheden dan de hierboven genoemde.

35. Tot slot wijst de Autoriteit erop dat de wenselijkheid van het instellen van onderzoeken *in concreto* moet worden beoordeeld door de inspecteurs op basis van de feiten waarover zij beschikken. Zij beschikken over een beoordelingsbevoegdheid in dit verband. De inspecteurs zullen de elektronische verzameling van de noodzakelijke gegevens oordeelkundig en met mate uitvoeren en alleen persoonsgegevens raadplegen indien ze, gelet op de feiten, beschikken over een samenhangende en ernstige reeks aanwijzingen dat de gewenste persoonsgegevens de preventie en opsporing van inbreuken op de Cyberbeveiligingsverordening of de certificeringsregeling waarvan de naleving wordt gecontroleerd, mogelijk zouden maken of zouden versnellen.

Mededeling door de inspectiedienst van zijn inspectieverslagen en pv's van controle aan derden

36. Artikel 16, § 2, van het voorontwerp van wet bepaalt dat de nationale cyberbeveiligingscertificeringsautoriteit of de overheid die door de Koning is aangewezen krachtens artikel 5, § 2, van het voorontwerp van wet, een afschrift van haar inspectieverslag meedeelt aan de *"markttoezichtautoriteiten, de nationale accreditatieautoriteit, de openbare*

[10] Zie hierover ENISA: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases en https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation.

veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid, op hun verzoek en voor zover dit nodig is voor het vervullen van hun wettelijke opdrachten."

37. Om de in de algemene opmerkingen van dit advies uiteengezette redenen ziet de Autoriteit niet in waarom een dergelijke openbaarmaking op eenvoudig verzoek gepast is voor de inlichtingendiensten, de openbare veiligheidsdiensten en de politiediensten voor de goede uitvoering van de Cyberbeveiligingsverordening. Ondervraagd over dit onderwerp, verklaarde de afgevaardigde van de minister het volgende: *"La transmission d'une copie d'un rapport d'inspection ou d'un procès-verbal relatif au contrôle d'un certificat de cybersécurité par l'une des autorités précitées peut s'avérer nécessaire à l'exécution des missions légales de ces autorités ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique."* Hij haalde de bestaande wettelijke bepalingen aan op grond waarvan bepaalde autoriteiten, zoals het Nationaal Crisiscentrum of het OCAD, over dit soort informatie kunnen beschikken. In dit verband merkt de Autoriteit in de eerste plaats op dat de auteur van het voorontwerp van wet ervoor moet zorgen dat niet in vage bewoordingen wordt voorzien in gegevensstromen die reeds door andere wettelijke bepalingen worden geregeld. Bovendien valt het niet binnen de doelstellingen of het toepassingsgebied van het voorontwerp van wet om de inspectiebevoegdheden te regelen van andere overheidsautoriteiten dan die welke belast zijn met het toezicht op de naleving van de Europese verordening en de op grond van die verordening vastgestelde certificeringsregelingen. Om de evenredigheid van deze ontwerpbepaling te waarborgen, moeten vervolgens de voor de uitvoering van de Europese Cyberbeveiligingsverordening legitieme en relevante omstandigheden en doeleinden waarin de bedoelde verslagen mogen worden meegedeeld aan uitsluitend de autoriteiten met specifieke openbaredienstopdrachten op het gebied van cyberbeveiliging, duidelijk worden bepaald in het voorontwerp van wet, in plaats van te voorzien in mededelingen op eenvoudig verzoek, zonder enige andere precisering en onverminderd andere wettelijke bepalingen op grond waarvan overheidsautoriteiten toegang kunnen krijgen tot bepaalde verslagen of bepaalde daarin vervatte inlichtingen.

38. Bovendien moet, naar het voorbeeld van wat reeds is aanbevolen, duidelijk worden gemaakt dat deze verslagen geen persoonsgegevens over klanten (of klanten van die klanten) van de gecontroleerde ICT-dienstverleners mogen bevatten vanwege de risico's die dit voor deze betrokkenen inhoudt. Voor het overige verwijst de Autoriteit naar haar algemene overwegingen hierboven. De formulering van het artikel 16, § 2 van het ontwerp moet dienovereenkomstig worden herzien.

39. Artikel 16, § 3, van het voorontwerp bepaalt de geadresseerden aan wie deze inspectieverslagen systematisch moeten worden toegezonden in geval van een *"controle bij een kritieke infrastructuur, een aanbieder van essentiële diensten of een digitaledienstverlener als bedoeld in 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 of het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer".*

40. Daarmee voert het voorontwerp van wet een wettelijke verplichting in om persoonsgegevens te verwerken (ervan uitgaande dat deze rapporten persoonsgegevens zullen bevatten of betrekking zullen hebben op een dienstverlener/leverancier van ICT-diensten/-producten die als natuurlijk persoon opereert) in de zin van artikel 6.1.c van de AVG. Aangezien de specifieke wetgevingen bedoeld in artikel 16, § 3 van het ontwerp een gelijkaardig doel nastreven als de Cyberbeveiligingsverordening, heeft de Autoriteit geen bezwaar tegen de mededeling van verslagen in het geval dat een inspectie door de in artikel 5 van het voorontwerp van wet bedoelde autoriteiten betrekking heeft op entiteiten die gebruik maken van de genoemde ICT-diensten of -producten bedoeld in de wetgevingen zoals vermeld in artikel 16, § 3. In een streven naar rechtszekerheid en voorzienbaarheid en om te voldoen aan artikel 6.3 van de AVG moet het begrip *"bevoegde sectorale autoriteit en inspectiedienst"* echter adequaat worden gedefinieerd, moet in artikel 16, § 3, het precieze doel worden vastgesteld waarvoor deze ontvangende autoriteiten deze verslagen zullen gebruiken (namelijk de uitoefening van hun bij de genoemde specifieke reglementeringen opgelegde openbaredienstopdrachten) en moet worden gespecificeerd dat de verslagen uitsluitend mogen worden gericht aan de bevoegde sectorale autoriteit op basis van de dienstverlener of leverancier van de ICT-dienst waarop het verslag betrekking heeft.

41. Artikel 17, §§ 1 tot 4, van het voorontwerp bepaalt op zeer ruime wijze de mededeling aan derden van gegevens en processen-verbaal van controle door de inspectiedienst van de nationale certificeringsautoriteit.

42. De formulering *"die ervan op de hoogte moeten zijn (...) voor de uitoefening van hun functie of opdracht die verband houdt met deze wet of andere wettelijke bepalingen"* artikel 17, § 1 van het ontwerp is een vaag en te ruim criterium om de verstrekking van door de inspectiedienst verzamelde persoonsgegevens aan andere autoriteiten te regelen, temeer daar § 2 van artikel 17 van het ontwerp de inspectiedienst onderwerpt aan het beroepsgeheim. Bijgevolg moet dit artikel 17, § 1 worden geschrapt.

43. Met betrekking tot artikel 17, § 3 van het ontwerp, dat voorziet in de mededeling door de inspectiedienst van pv's of aanvullende informatie aan de verschillende bedoelde autoriteiten, verwijst de Autoriteit naar het commentaar in de algemene opmerkingen in dit advies en naar het commentaar bij artikel 16, § 2 van het ontwerp, die *mutatis mutandis* van toepassing zijn. Evenzo wordt voor artikel 17, § 4 verwezen naar het commentaar bij artikel 16, § 3.

Afwijking van het beginsel van vertrouwelijkheid van elektronische communicatie ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit

44. Artikel 17, § 5 van het ontwerp voorziet als volgt in een afwijking van het beginsel van vertrouwelijkheid van communicatie via een openbaar netwerk en een openbare elektronisch-communicatiedienst[11] ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit:
"§ 5. Bij de uitoefening van hun functie mogen de personeelsleden van de inspectiedienst:
1° met opzet kennisnemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hen bestemd is;
2° met opzet de personen identificeren die bij de overdracht van de informatie en de inhoud ervan betrokken zijn;
3° met opzet kennisnemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon."

45. Binnen de grenzen van artikel 15 van de richtlijn betreffende privacy en elektronische communicatie kan in dergelijke afwijkingen worden voorzien. Artikel 15.1 van de richtlijn betreffende privacy en elektronische communicatie bepaalt: *"De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, [...] en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de*

[11] vastgelegd in artikel 5, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), in Belgisch recht omgezet in artikel 124 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Europese Unie."[12] Met de inwerkingtreding van de AVG moet artikel 15 van de richtlijn betreffende privacy en elektronische communicatie worden gelezen als een verwijzing naar artikel 23 van de AVG. Deze bepaling van de AVG voorziet onder meer als een grond voor beperking van de rechten van betrokkenen in *"een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen"*; met name de veiligheid en de landsverdediging, de openbare veiligheid, de voorkoming en de opsporing van strafbare feiten, andere belangrijke doelstellingen van algemeen openbaar belang, met name een belangrijk economisch of financieel belang, en de voorkoming en de opsporing van schendingen van de beroepscodes voor gereglementeerde beroepen.

46. Allereerst is het aan de auteur van het voorontwerp van wet om in de memorie van toelichting uit te leggen hoe de voorgestelde afwijking ten behoeve van de inspectiedienst van de nationale cyberbeveiligingscertificeringsautoriteit aansluit bij een of meer van de gronden van artikel 23.1 van de AVG.

47. Vervolgens vraagt de Autoriteit zich af, gelet op de gronden waarop de lidstaten van dit vertrouwelijkheidsbeginsel kunnen afwijken, of het in dit geval niet passend zou zijn deze afwijkingen te beperken tot de controles die moeten worden uitgevoerd bij conformiteitsbeoordelingsinstanties en houders van verplichte certificaten, aangezien er op gebieden van groot openbaar belang wetgevende maatregelen zouden moeten worden genomen om dergelijke certificaten verplicht te stellen. Het is aangewezen dat de auteur van het voorontwerp van wet de keuze die hij zal maken voor het toepassingsgebied van de afwijking, vanuit deze invalshoek motiveert en zijn motivering in de memorie van toelichting opneemt.

48. Gevraagd naar de behoeften van de inspectiedienst die een dergelijke afwijking van het beginsel van vertrouwelijkheid van elektronische communicatie vereisen, heeft de afgevaardigde van de minister het volgende verklaard: *"Ne sont pas visées les écoutes téléphoniques mais la* (prise de connaissance) *des e-mails émanant et reçus des organismes d'évaluation de la conformité, des émetteurs de déclaration de conformité, des titulaires de certificat de cybersécurité européen et ce uniquement lorsque les données en question sont susceptibles de contribuer à l'élucidation d'un manquement grave à un schéma de certification dont le respect est contrôlé."*

[12] Artikel 6, §§ 1 en 2, van het Verdrag betreffende de Europese Unie luidt als volgt: "1. De Unie erkent de rechten, vrijheden en beginselen die zijn vastgesteld in het Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg, dat dezelfde juridische waarde als de Verdragen heeft [...]." Uit de rechtspraak van het HvJEU volgt dat alle in artikel 23 (oud artikel 13 van richtlijn 95/46) van de AVG genoemde rechtvaardigingsgronden een afwijking van dit beginsel van vertrouwelijkheid van elektronische communicatie kunnen rechtvaardigen.

49. Om het proportionele karakter van de afwijking te waarborgen, is het dus aan de auteur van het wetsontwerp om in artikel 17, § 3 van het ontwerp te specificeren dat de inspecteurs enkel kennis kunnen nemen van elektronische communicatie die uitgaat van en ontvangen wordt door conformiteitsbeoordelingsinstanties (verstrekkers van conformiteitsverklaringen)[13], houders van het (verplichte) Europese cyberbeveiligingscertificaat[14], en enkel indien deze informatie waarschijnlijk zal bijdragen tot het ophelderen van een ernstige inbreuk op een gecontroleerde (verplichte) certificeringsregeling of op de Europese Cyberbeveiligingsverordening. In een streven naar rechtszekerheid en voorzienbaarheid moet ook uitdrukkelijk worden vermeld dat artikel 17, § 3 afwijkt van artikel 124 van de voornoemde wet van 13 juni 2005.

50. Tot heeft de afgevaardigde van de minister op de vraag of het wenselijk was te voorzien in waarborgen voor de gecontroleerde personen, zoals hun voorafgaande instemming met de raadpleging van hun elektronische communicatie of, bij gebreke daarvan, de instemming van de onderzoeksrechter, het volgende gepreciseerd: *"En l'absence du consentement expresse de l'entité contrôlée, les membres assermentés du service d'inspection de l'autorité nationale de certification de cybersécurité ne pourront pas prendre connaissance de ces informations (ceux-ci n'ayant pas la qualité d'officier de police judiciaire)."*Daarom is het aangewezen om in artikel 17, § 3 van het ontwerp te bepalen dat de bedoelde raadplegingen plaatsvinden na het verkrijgen van de toestemming van de gecontroleerde persoon.

Hoofdstuk 8 – Verwerking van persoonsgegevens

51. De auteur van het wetsontwerp heeft ervoor gekozen in zijn voorontwerp van wet een specifiek hoofdstuk op te nemen waarin de verschillende elementen van de onder het voorontwerp van wet vallende verwerking van persoonsgegevens worden vastgesteld.

Categorieën van verwerking van persoonsgegevens en doeleinden van die verwerking

52. In artikel 36, §§ 1 en 3, worden de categorieën van verwerking van persoonsgegevens in het kader van de uitvoering van het voorontwerp als volgt omschreven:
"Art. 36, § 1. In het kader van de uitvoering van deze wet vinden de volgende verwerkingen van persoonsgegevens plaats:
1° informatie-uitwisseling tussen de autoriteit bedoeld in artikel 5, § 1, de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, de gerechtelijke overheden, de sectorale overheden of de inspectiediensten respectievelijk bedoeld 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

[13] Afhankelijk van de keuze die in het licht van de vorige overweging moet worden gemaakt.
[14] *Ibidem.*

belang voor de openbare veiligheid, de markttoezichtautoriteiten, de nationale accreditatieautoriteit, de openbare veiligheidsdiensten, de politiediensten, de inlichtingendiensten en de autoriteit bedoeld in artikel 7, § 4, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerken informatiesystemen van algemeen belang voor de openbare veiligheid;

(…)

2° informatie-uitwisseling tussen conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen, enerzijds, en de autoriteit bedoeld in artikel 5, § 1, of de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, anderzijds;

(…)

3° de verwerking van gegevens door de autoriteit bedoeld in artikel 5, § 1, of door een conformiteitsbeoordelingsinstantie, voor het vervullen van de in hoofdstuk 7 bedoelde taken rond klachten.

(...);

4° de verwerking van gegevens door de autoriteit bedoeld in artikel 5, § 1, of door de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, met betrekking tot haar taken op het vlak van toezicht en sancties.

(…)

§ 3. 2. De in paragraaf 1 bedoelde verwerkingen vinden plaats voor de volgende doeleinden:

1° de afgifte van Europese cyberbeveiligingscertificaten;

2° het toezicht op houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of conformiteitsbeoordelingsinstanties;

3° de verwerking van klachten ingediend op basis van artikel 63, lid 1, van de Cyberbeveiligingsverordening;

4° nationale en internationale samenwerking, met inbegrip van informatie-uitwisseling;

5° het opleggen van de sancties bedoeld in hoofdstuk 6."

53. Ten eerste merkt de Autoriteit op dat het begrip *"verwerking van persoonsgegevens in het kader van de uitvoering van deze wet"* niet voldoet aan de eisen van voorzienbaarheid. Gelet op het toepassingsgebied van het voorontwerp van wet is het aangewezen om alleen de verwerking van persoonsgegevens te regelen die door de nationale cyberbeveiligingscertificeringsautoriteit en, in voorkomend geval, de ter uitvoering van artikel 5, § 2 van het voorontwerp van wet aangewezen autoriteiten (voor zover deze laatste verwerkingen niet reeds door de organieke wetten van deze autoriteiten worden geregeld) zal worden verricht bij de uitvoering van de in de Europese Cyberbeveiligingsverordening beschreven openbaredienstopdrachten die het voorontwerp van wet hun toekent. Het voorontwerp van wet mag geen gegevensverwerkingen regelen die buiten dit toepassingsgebied vallen of die bovendien reeds zijn geregeld door de organieke wetten van andere autoriteiten; het is aan de auteur van het voorontwerp van wet om dit na te gaan.

54. Een uitputtende beschrijving van de gegevensverwerkingscategorieën die ter uitvoering van het wetsontwerp worden verricht, zoals artikel 36, § 1 van het ontwerp poogt te doen, zou afbreuk kunnen doen aan de uitoefening van de openbaredienstopdrachten van de nationale certificeringsautoriteit in het geval er sprake zou zijn van een vergetelheid. Een duidelijke en

concrete vaststelling van de doeleinden van de verwerkingen van deze autoriteit (naast de vaststelling van de andere essentiële elementen ervan) moet volstaan om de noodzakelijke voorzienbaarheid van deze verwerkingen van persoonsgegevens te waarborgen. De Autoriteit beveelt de schrapping van artikel 36, § 1 aan.

55. Wat de bepaling van de doeleinden van de verwerkingen in artikel 36, § 3 van het ontwerp betreft, moet worden verwezen naar de doeleinden waarvoor de nationale certificeringsautoriteit en/of de autoriteiten die ter uitvoering van artikel 5, § 2 van het voorontwerp van wet zullen worden aangewezen, persoonsgegevens zullen verwerken in het kader van de openbaredienstopdrachten die hun worden toegekend door het voorontwerp van wet en de Europese Cyberbeveiligingsverordening[15]. De volgende opmerkingen zijn in dit verband op hun plaats:
    a. De in artikel 36, § 3, 1° en 3°, genoemde doeleinden moeten op nuttige wijze worden samengevoegd: de afgifte van Europese cyberbeveiligingscertificaten en het beheer van de daarmee verband houdende klachten;
    b. De doeleinden bedoeld in artikel 36, §3, 2° en 5° moeten eveneens worden samengevoegd en er moet worden verwezen naar de relevante bepalingen van het voorontwerp van wet in de volgende bewoordingen: toezicht op houders van een Europese cyberbeveiligingscertificaat, verstrekkers van conformiteitsverklaringen van de Europese Unie en conformiteitsbeoordelingsinstanties en, in voorkomend geval, het opleggen van sancties in overeenstemming met de hoofdstukken 5 en 6 van deze wet;
    c. Wat de "samenwerking, met inbegrip van de uitwisseling van informatie op nationaal en internationaal niveau" betreft, dit is geen verwerkingsdoel in de zin van de AVG, maar een gegevensverwerking op zich die reeds moet worden gedekt door de bovengenoemde controle- en sanctiedoeleinden en, indien nodig en overeenkomstig de Cyberbeveiligingsverordening, door het doel van *"afgifte van certificaten"*. Artikel 36, § 3, 4° moet bijgevolg worden geschrapt en, in voorkomend geval, indien de bestaande wettelijke bepalingen (NIS-wet) niet reeds op voorzienbare wijze voorzien in deze stromen, moet deze bepaling van het ontwerp worden vervangen door het concrete doel waarvoor een mededeling van informatie door de nationale certificeringsautoriteit en de ter uitvoering van artikel 5, § 2 van het ontwerp aangewezen autoriteiten alleen zal worden gedaan aan de bevoegde sectorale autoriteiten (NIS), in overeenstemming met de artikelen 16 en 17 van het voorontwerp van wet (aangepast in overeenstemming met de bovenvermelde aanbevelingen van de Autoriteit). Indien de auteur van het voorontwerp van wet de nationale cyberbeveiligingscertificeringsautoriteit wil laten deelnemen aan de internationale samenwerking om de kwaliteit van de certificeringen te

[15] Artikel 36 van het ontwerp is momenteel gericht op het reguleren van *"gegevensverwerking in het kader van de uitvoering van de wet"*. Niet alle gegevensverwerkingen die worden uitgevoerd als doel *"de afgifte van Europese cyberbeveiligingscertificaten"* vallen echter, terecht, onder het voorontwerp van wet. De formulering van artikel 36 van het ontwerp moet bijgevolg in dit opzicht worden herzien.

verbeteren en de benaderingen op dit gebied te harmoniseren, en indien voor een dergelijke samenwerking een uitwisseling van persoonsgegevens tussen de nationale cyberbeveiligingscertificeringsautoriteiten vereist is, is het aangewezen dat een dergelijk doel concreet en nauwkeurig wordt vermeld.

Kwalificatie van de verwerkingsverantwoordelijke

56. Om elke dubbelzinnigheid over de identiteit van de entiteit die moet worden beschouwd als verwerkingsverantwoordelijke te vermijden, en aldus de uitoefening van de rechten van de betrokkene waarin de artikelen 12 tot en met 22 van de AVG voorzien, te vergemakkelijken, verzoekt de Autoriteit de auteur van het voorontwerp van wet om de verwerkingsverantwoordelijke(n) explicieter te identificeren dan in artikel 36, § 1 van het ontwerp het geval is.

57. Daartoe volstaat de precisering dat de nationale cyberbeveiligingscertificeringsautoriteit de verantwoordelijke is voor de verwerkingen die zij uitvoert voor de in artikel 36, § 3 genoemde doeleinden. Hetzelfde geldt voor de in artikel 5, § 2 van het voorontwerp bedoelde autoriteiten met betrekking tot de verwerkingen die worden verricht voor in de hoofdstukken 5 en 6 van het voorontwerp van wet bedoelde toezicht- en sanctiedoeleinden.

Rechtsgrondslag

58. In artikel 36, § 2 van het ontwerp wordt de rechtsgrondslag van de bedoelde verwerkingen als volgt omschreven:
"§ 2. De in paragraaf 1 bedoelde verwerkingen zijn noodzakelijk om te voldoen aan wettelijke verplichtingen van de Cyberbeveiligingsverordening of van deze wet, of om een taak van algemeen belang te vervullen die is opgedragen aan een van de in deze wet bedoelde overheden."

59. De Autoriteit merkt op dat de meeste verwerkingen van persoonsgegevens waarop het voorontwerp van wet betrekking heeft, verwerkingen zullen zijn die door de nationale cyberbeveiligingscertificeringsautoriteit (en de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten) worden uitgevoerd bij de uitvoering van hun openbaredienstopdrachten; de rechtsgrondslag, in de zin van de AVG, is artikel 6.1.e van de AVG (met uitzondering van de verplichte systematische verstrekking van inspectieverslagen en processen-verbaal waarin is voorzien in artikel 16, § 3 en artikel 17, § 4 van het voorontwerp van wet, waarvan de rechtsgrondslag artikel 6.1.c van de AVG is).

60. Artikel 36, § 2 van het ontwerp voegt geen meerwaarde toe wat de voorzienbaarheid van de bedoelde gegevensverwerkingen betreft. Om de rechtmatigheid en voorzienbaarheid van

verwerkingen op grond van artikel 6.1.e van de AVG te waarborgen, moet een rechtstreeks toepasselijke nationale of supranationale rechtsnorm op voldoende duidelijke en nauwkeurige wijze de openbaredienstopdrachten die aan de verwerkingsverantwoordelijke zijn toevertrouwd, vaststellen (wat het geval is in het voorontwerp van wet en de Europese Cyberbeveiligingsverordening), maar het is niet vereist dat deze norm of de nationale norm ter uitvoering van een Europese verordening specificeert dat de gegevensverwerkingen die voor dit doel worden uitgevoerd, plaatsvinden *"ter uitvoering van een openbaredienstopdracht die aan de verwerkingsverantwoordelijke is toevertrouwd".* Bijgevolg moet dit artikel 36, § 2 van het ontwerp worden geschrapt.

Categorieën van verwerkte persoonsgegevens

61. In artikel 36, § 4 worden de categorieën van verwerkte persoonsgegevens als volgt omschreven:
"§ 4. De verwerkte persoonsgegevens zijn identificatie- of authenticatiegegevens en elektronischecommunicatiegegevens.
Na advies van de autoriteit bedoeld in artikel 5, § 1, of van de overheid die voor de opdrachten bedoeld in hoofdstuk 5 en 6 door de Koning is aangewezen, kan de Koning het vorige lid aanvullen met andere persoonsgegevens."

62. Afgezien van het feit dat in het voorontwerp van wet niet wordt gespecificeerd door welke entiteit deze gegevenscategorieën worden verwerkt, biedt deze vaststelling geen meerwaarde wat de voorzienbaarheid van de gegevensverwerkingen in kwestie betreft. Bovendien is de Autoriteit, in toepassing van het legaliteitsbeginsel, van oordeel dat het in dit geval niet aan de Koning kan worden gedelegeerd om de lijst aan te vullen van de categorieën van persoonsgegevens die zullen moeten worden verwerkt door de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die ter uitvoering van artikel 5, § 2 van het voorontwerp van wet zijn aangewezen voor de uitvoering van de openbaredienstopdrachten die het voorontwerp van wet hun toevertrouwt. Aangezien de huidige lijst duidelijk onvolledig is (quid met de gegevens over de deskundigheid of de opleiding van het personeel van de dienstverlener die gecertificeerd is of bezig is met de certificeringsprocedure?), moet ze worden aangevuld in het licht van de gemeenschappelijke criteria (common criteria)[16] op dit gebied en moet de inhoud ervan naar behoren worden verantwoord en gemotiveerd in de memorie van toelichting.

[16] De gemeenschappelijke criteria voor de evaluatie van de beveiliging van IT-technologieën (bekend als de Common Criteria of CC) zijn een internationale norm (ISO/IEC 15408) voor de certificering van IT-beveiliging.

63. Wat de gegevenscategorieën betreft die worden verwerkt ter uitvoering van de hoofdstukken 5 en 6 van het voorontwerp van wet (toezicht en sanctie), erkent de Autoriteit dat het niet mogelijk is deze anders dan op functionele wijze vast te stellen, door te specificeren dat het gaat om gegevens die noodzakelijk zijn voor de uitoefening van de in de hoofdstukken 5 en 6 van het voorontwerp bedoelde toezicht- en sanctietaken.

64. Bijgevolg moet artikel 36, § 4 uit het voorontwerp van wet dienovereenkomstig worden herzien.

Categorieën van natuurlijke personen ten aanzien van wie gegevens worden verwerkt

65. Artikel 36, § 5 bepaalt in deze bewoordingen de categorieën van personen ten aanzien van wie gegevens worden verwerkt voor de hierboven genoemde doeleinden:
"§ 5. De persoonsgegevens van de volgende categorieën van personen kunnen het voorwerp uitmaken van de in paragraaf 1 bedoelde verwerkingen:
1° iedere persoon die optreedt voor conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten, afgevers van EU-conformiteitsverklaringen of voor een overheid;
2° iedere persoon die deelneemt aan een controle of verhoor in het kader van de toezichtsopdrachten bedoeld in hoofdstuk 5;
3° iedere persoon die een klacht indient."

66. In de eerste plaats moet worden verwezen naar natuurlijke personen, en niet gewoon naar personen.

67. Ten tweede vraagt de Autoriteit zich af of deze opsomming misschien onvolledig is in het licht van haar algemene opmerkingen aan het begin van het advies. Als dit het geval is, moet dit worden verholpen en, als waarborg voor de bescherming van de rechten en vrijheden van de klanten (of de klanten van die laatsten) van de dienstverleners/leveranciers van ICT-producten en in overeenstemming met de algemene overwegingen van de Autoriteit zoals uiteengezet aan het begin van het advies, is het van belang te specificeren dat de nationale cyberbeveiligingscertificeringsautoriteit en de krachtens artikel 5, § 2 van het ontwerp aangewezen autoriteiten geen gegevens mogen verwerken met betrekking tot natuurlijke personen-klanten (of klanten van die laatsten) van de onder toezicht staande dienstverleners/leveranciers van ICT-producten voor andere doeleinden dan het toezicht op de naleving door deze dienstverleners/leveranciers van de Europese Cyberbeveiligingsverordening en de Europese certificeringsregelingen waarop het toezicht betrekking heeft.

Bewaartermijn

68. Artikel 39 bepaalt de bewaartermijn van de krachtens het voorontwerp van wet verzamelde gegevens in de volgende bewoordingen:
"Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening EU 2016/679, bewaart de verwerkingsverantwoordelijke de in uitvoering van de wet verwerkte persoonsgegevens, onverminderd eventuele beroepsprocedures, gedurende 10 jaar na afloop van de verwerking die is uitgevoerd om een van de doeleinden bedoeld in artikel 36, § 3, te realiseren."

69. Zoals hierboven reeds is uiteengezet, moet de bewaartermijn van de persoonsgegevens die worden verzameld door de nationale cyberbeveiligingscertificeringsautoriteit en de ter uitvoering van artikel 5, § 2 van het project aan te wijzen autoriteiten voor de verwezenlijking van de in artikel 36, § 3 beoogde doeleinden, worden vastgesteld. De formulering van artikel 39 van het ontwerp moet nuttig worden aangepast in die zin.

70. Wat de beoogde bewaartermijn betreft, heeft de Autoriteit geen opmerkingen.

Afwijking van de rechten van de betrokkenen

71. Artikel 37 van het voorontwerp van wet wijkt in zeer ruime mate af van alle rechten van de betrokkenen krachtens de AVG.

72. Elke beperking van de rechten van betrokkenen krachtens de AVG moet niet alleen een van de in artikel 23.1 van de AVG genoemde doeleinden nastreven, maar ook voldoen aan de in artikel 23.2 van de AVG voorgeschreven vormen. Bovendien moet elke beperking van de rechten van de betrokkenen ook beperkt blijven tot wat strikt noodzakelijk is, zowel wat de reikwijdte als wat de duur betreft[17].

73. In de eerste plaats moeten de verwerkingsverantwoordelijke(n) die deze afwijkingen genieten, uitdrukkelijk worden vermeld, namelijk, zoals blijkt uit de aanvullende informatie, de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten die ter uitvoering van het artikel 5, § 2 van het ontwerp zullen worden aangewezen.

---

[17] Advies nr. 34/2018 van 11 april 2018 *over een voorontwerp van wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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*, meer bepaald de overwegingen 36 tot 38; Advies nr. 41/2018 van 23 mei 2018 *over een voorontwerp van wet houdende diverse financiële bepalingen*; Advies nr. 88/2018 van 26 september 2018 *over het ontwerp van besluit van de Vlaamse Regering houdende aanpassing van de besluiten van de Vlaamse Regering aan de verordening (EU).*

74. Volgens artikel 37 van het ontwerp komen de verwerkingen van de genoemde verantwoordelijken waarvoor de beoogde afwijking zal gelden, overeen met de verwerkingen die worden verricht met als doel het beheer van klachten in verband met de toekenning van een cyberbeveiligingscertificaat of de weigering om een dergelijk certificaat af te geven.

75. Hoewel de Autoriteit begrijpt dat er voor controleverwerkingen moet worden voorzien in afwijkingen van bepaalde door de AVG gewaarborgde rechten (om deze controleverrichtingen niet in het gedrang te brengen), vraagt zij zich af of het nodig is in dit soort afwijkingen te voorzien voor het beheer van klachten in verband met de toekenning of de weigering van certificaten. Wat de laatstgenoemde verwerkingen betreft, kan de Autoriteit anderzijds begrijpen dat het nodig is in het voorontwerp van wet te voorzien in de mogelijkheid voor klagers om te verzoeken dat hun klacht zodanig wordt behandeld dat hun anonimiteit wordt bewaard (voor zover de behandeling van de klacht dit toelaat), maar afgezien van dit geval, dat in het voorontwerp van wet kan worden opgenomen, lijkt het in het licht van de verkregen aanvullende inlichtingen niet nodig te voorzien in een afwijking van de in de artikelen 12 tot 22 van de AVG bedoelde rechten om te garanderen dat klachten naar behoren worden verwerkt. Bij gebrek aan een relevante rechtvaardiging in de memorie van toelichting moet het toepassingsgebied van de afwijking dienovereenkomstig worden beperkt.

76. Vervolgens, met betrekking tot de afwijking ten behoeve van de gegevensverwerkingen door de inspectiediensten met als doel de uitoefening van hun controle-opdrachten zoals bedoeld in artikel 13 van het voorontwerp van wet, merkt de Autoriteit op dat het ter toepassing van artikel 23.2 van de AVG aan de auteur van het voorontwerp van wet is om in artikel 37 van het ontwerp de reikwijdte van de beperkingen te specificeren, niet alleen op het vlak van rechten waarvan wordt afgeweken, maar ook op het vlak van limieten van de beoogde afwijking, in plaats van te bepalen: *"De uitzondering geldt enkel indien en voor zover deze verwerkingen noodzakelijk zijn voor de hierboven bepaalde doeleinden, met name voor zover de toepassing van de rechten waarin deze verordening voorziet nadelig zou zijn voor een controle, onderzoek of klacht"*; wat de vereiste rechtszekerheid op dit vlak niet ten goede komt.

77. In dit verband beveelt de Autoriteit aan, zonder exhaustief te willen zijn, te specificeren dat de afwijkingen van de rechten van de betrokkenen alleen gelden gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of een onderzoek (met inbegrip van voorbereidende handelingen tot één jaar na ontvangst van het verzoek om uitoefening van het recht[18]) en gedurende de periode die nodig is voor de vervolging ter zake, voor zover de

[18] Teneinde te zorgen voor een redelijke beperking in de tijd voor de afwijking.

uitoefening van de rechten afbreuk zou doen aan de behoeften van de controle, het onderzoek of de voorbereidende handelingen.

78. Wat de keuze betreft van de artikelen van de AVG waarvan in het voorontwerp van wet voor de uitoefening van de inspectie-opdracht wordt besloten af te wijken, dienen de volgende opmerkingen te worden gemaakt:
    a. Artikel 12 van de AVG vermeldt uitdrukkelijk de transparantie van informatie en communicatie en de modaliteiten voor de uitoefening van de rechten van de betrokkenen en vormt op zich geen recht van de betrokkenen. Er is geen reden om hiervan af te wijken.
    b. Het is niet nodig om voor het beoogde doel af te wijken van het recht op gegevenswissing (art. 17 AVG). Hierover ondervraagd specificeerde de afgevaardigde van de minister het volgende: *"Il est prévu que les données à caractère personnel soient conservées sans préjudice de recours éventuels, par le responsable du traitement 10 ans suivant la fin du traitement effectué afin d'atteindre une des finalités visées à l'article 36, § 3. Cette durée se justifie par la nécessité de s'assurer de conserver plus longtemps les données à caractère personnel pouvant être liées à un faux ou usage de faux relatif à une certification de cybersécurité. Le service d'inspection doit également pouvoir d'identifier les cas de récidive pour les mêmes faits dans un délai de trois ans (qui peuvent donner lieu au doublement de l'amende administrative en vertu de l'article 24, § 4 de l'avant-projet). Or, sur base du droit à l'effacement, la personne concernée pourrait obtenir l'effacement prématuré de ses données. Il apparaît donc nécessaire de limiter ce droit."* In dit verband merkt de Autoriteit op dat betrokkenen op grond van het recht op gegevenswissing niet kunnen verkrijgen dat hun gegevens voortijdig worden gewist, maar uitsluitend wanneer een van de in artikel 17 genoemde gronden van toepassing is, wat in casu geen belemmering lijkt voor de controleprocedure van de inspectiedienst. We wijzen er ook op dat de diensten van de sociale inspectie en de fiscale inspectie evenmin van dit recht mogen afwijken, hoewel de redenen voor hun afwijkingen van de rechten van de betrokkenen in de AVG dezelfde zijn. Daarom moet de afwijking van dit recht uit artikel 37 van het ontwerp worden geschrapt.
    c. In dezelfde geest als het bovenstaande moet ook de afwijking van het recht van verzet om dezelfde redenen uit artikel 37 van het ontwerp worden geschrapt. In artikel 21 van de AVG wordt bepaald dat wanneer een betrokkene bezwaar maakt tegen verwerking van zijn gegevens ten behoeve van de uitoefening van een openbaredienstopdracht, *"de verwerkingsverantwoordelijke [...] de verwerking van de persoonsgegevens [staakt] tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering"*; wat voor de certificeringsautoriteit moeilijk te bewijzen zal zijn in het geval dat een dergelijk recht

wordt uitgeoefend door een gecontroleerde persoon; wat trouwens erg onwaarschijnlijk is aangezien een betrokkene dit recht pas kan uitoefenen wanneer hij er kennis van heeft dat hij wordt gecontroleerd; wat niet het geval zal zijn aangezien afgeweken wordt van de rechten op informatie en toegang.

d. Wat de afwijking van artikel 22 van de AVG door artikel 37 van het ontwerp betreft, betoogde de afgevaardigde van de minister in dit verband het volgende: *"Des décisions individuelles automatisées (fondées sur l'utilisation d'algorithmes) en matière de contrôle et de sanctions ne sont pas prévues à ce stade mais leur utilisation pourrait s'avérer dans le futur utile ou nécessaire."* In overeenstemming met artikel 22.2 van de AVG moeten, opdat de in artikel 5 van het voorontwerp van wet bedoelde autoriteiten, uitsluitend op basis van geautomatiseerde verwerking besluiten zouden kunnen nemen die rechtsgevolgen hebben voor de betrokkenen of hen ingrijpend treffen, deze besluiten worden genomen op grond van een specifieke wettelijke bepaling die de geautomatiseerde besluiten regelt en voorziet in passende maatregelen om de rechten en vrijheden van de betrokkenen te beschermen; dit is niet het geval in het voorontwerp van wet dat ter advies is voorgelegd. De afwijking van artikel 22 van de AVG lijkt bijgevolg niet nodig en moet eveneens worden weggelaten.

e. Artikel 20 van de AVG moet ook worden geschrapt van de lijst van artikelen waarvan wordt afgeweken, aangezien het in casu toch niet van toepassing is, zoals de afgevaardigde van de minister heeft bevestigd.

79. Teneinde artikel 37 van het ontwerp verenigbaar te maken met artikel 23.2 van de AVG moet bovendien worden voorzien in soortgelijke garanties als die waarin hoofdstuk 5/1 van het Sociaal Strafwetboek voorziet, aangezien de genoemde afwijkingen en garanties voor de rechten en vrijheden van de betrokkenen reeds zijn goedgekeurd door de gegevensbeschermingsautoriteit[19] (opname van de functionaris voor gegevensbescherming bij de autoriteiten zoals bedoeld in artikel 5 van het ontwerp voor de vastlegging van de feitelijke of juridische gronden waarop het besluit tot weigering van het recht van de betrokkene is gebaseerd en terbeschikkingstelling van deze gronden aan de Gegevensbeschermingsautoriteit op haar eerste verzoek, het in kennis stellen van de betrokkenen van de afwijzing van hun verzoek en de redenen daarvoor, tenzij dit het doel van de controle in gevaar zou brengen, en het in kennis stellen van de betrokkenen die hun rechten hebben willen uitoefenen van de opheffing van de afwijking na de afronding van de controle, het in kennis stellen van de betrokkenen van de rechtsmiddelen waarover ze in dat verband beschikken, ...).

[19] Ibidem.

80. De Autoriteit ziet de relevantie van het artikel 37, § 4 van het ontwerp niet in. Bovendien biedt het niet de rechtszekerheid die voor een afwijking van een grondrecht vereist is. De schrapping ervan wordt aanbevolen.

81. Artikel 37, § 5 moet eveneens worden geschrapt aangezien het overbodig is ten opzichte van andere bepalingen van het voorontwerp van wet en geen verband houdt met de vereisten van artikel 23.2 van de AVG.

Afwijking van artikel 20 van de WVP

82. Artikel 38 voorziet in een afwijking van de verplichting om de doorgifte van persoonsgegevens door middel van een protocol te formaliseren, zowel voor de autoriteiten die gegevens zullen meedelen aan de cyberbeveiligingscertificeringsautoriteit en aan de in artikel 5, § 2 van het voorontwerp van wet bedoelde autoriteiten, als voor laatstgenoemden.

83. De Autoriteit herinnert eraan dat de verplichting om een gegevensuitwisseling te formaliseren zoals bedoeld in artikel 20 van de WVP niet geldt voor een punctuele mededeling van gegevens[20]; dit zou het geval zijn bij de toepassing van artikel 29 van de Sv. (gerechtelijke autoriteiten).

84. De norm, om te kunnen afwijken van artikel 20 van de WVP, moet een kader bieden voor de bedoelde structurele stroom van persoonsgegevens, op voorzienbare wijze en in overeenstemming met de beginselen van noodzakelijkheid en evenredigheid; dit vereist dat *"uitdrukkelijk wordt bepaald aan wie (ontvanger(s)) wat (categorieën van meegedeelde gegevens), wanneer en waarom (doeleinden en modaliteiten van de mededeling) wordt verstrekt* "[21], in overeenstemming met de beginselen van noodzakelijkheid en evenredigheid; dit moet gebeuren op het niveau van de bepalingen van het wetsontwerp die een kader bieden voor deze mededelingen van gegevens door de nationale autoriteit voor de certificering van cyberbeveiliging. In dit verband wordt verwezen naar de bovengenoemde opmerkingen van de Autoriteit over de artikelen 16 en 17 van het voorontwerp van wet, die een kader bieden voor deze structurele mededeling van gegevens.

85. De structurele verzamelingen van persoonsgegevens die de nationale cyberbeveiligingscertificeringsautoriteit en de autoriteiten bedoeld in artikel 5, § 2, zouden verrichten bij de sectorale autoriteiten (cf. supra) voor de uitvoering van de openbaredienstopdrachten waarin de Cyberbeveiligingsverordening voorziet, moeten aan dezelfde

[20] Aanbeveling 02/2020 van de Autoriteit van 31 januari 2020 betreffende draagwijdte van de verplichting om een protocol te sluiten om de mededelingen van persoonsgegevens door de federale publieke sector te formaliseren, p. 17.

[21] Ibidem, p. 16.

voorzienbaarheidscriteria voldoen opdat deze sectorale autoriteiten zouden worden vrijgesteld van de formalisering ervan door middel van een protocol in de zin van artikel 20 van de WVP. Voor zover de normen die deze sectorale autoriteiten regelen, hier niet in voorzien (wat de auteur van het voorontwerp van wet moet nagaan), moeten de bovengenoemde modaliteiten van deze mededelingen in het onderhavige voorontwerp van wet worden opgenomen voor zover zij betrekking hebben op persoonsgegevens.

Om deze redenen
is de Autoriteit
van oordeel dat het voorontwerp van wet dat voor advies is voorgelegd, in de volgende zin moet worden aangepast:

1. Herziening van artikel 6 §§ 1 en 3, 7, 16 §§ 2 en 3, 17 § 1 en 3, 36 §§ 1 en 3, 4° en 38, die voorzien in de uitwisseling van gegevens, teneinde deze adequaat te beperken tot hetgeen strikt noodzakelijk en evenredig is in het licht van de doelstellingen van de Cyberbeveiligingsverordening of aanverwante openbaredienstopdrachten die rechtstreeks van invloed zijn op de cyberbeveiliging, in overeenstemming met de algemene overwegingen van het advies en de specifieke overwegingen met betrekking tot deze bepalingen van het ontwerp (overw. 6 tot 14 en 19, 20, 37, 40 , 43 , 55, 85);

2. Oplegging van een specifieke informatieplicht aan de nationale certificeringsautoriteit in overeenstemming met overweging 15;

3. Schrapping van de taak van de afgifte van certificaten uit het toepassingsgebied van de afwijking van de geheimhoudingsplicht en het beroepsgeheim (overw. 23);

4. Omkadering van de afwijkingen van de geheimhoudingsplicht die nodig zijn voor de uitvoering van inspectietaken door de nationale certificeringsinstantie en de in artikel 5, § 2 bedoelde autoriteiten, in overeenstemming met overweging 26;

5. Instelling van passende waarborgen voor de eventuele verzamelingen van gegevens die nodig zijn voor de uitoefening van deze inspectietaken en die onder het beroepsgeheim vallen, in overeenstemming met overweging 27;

6. Verduidelijking van artikel 13, § 2 betreffende het verzamelen van informatie door de inspectiedienst, in overeenstemming met overweging 31;

7. Toevoeging van waarborgen voor de vrijwaring van de rechten en vrijheden van de klanten (natuurlijke personen) van de onder toezicht staande ICT-dienstverleners (of de natuurlijke personen die klanten zijn van die klanten) met betrekking tot de rechtmatige inzamelingen en mededelingen van de inspectiedienst (overw. 33, 38, 67);

8. Oplegging van de naleving van het evenredigheidsbeginsel bij de uitoefening van inspectietaken (overw. 34);

9. Motivering van het noodzakelijke karakter van de afwijking van het vertrouwelijkheidsbeginsel

van elektronische communicatie en beperking van de afwijking tot strikt noodzakelijke gevallen, omkadering van deze afwijking, in overeenstemming met de overwegingen 49 en 50 (overw. 45 tot 50);

10. Schrapping van de beschrijving van de categorieën van verwerking van persoonsgegevens (overw. 53 en 54);

11. Rectificatie van de beschrijving van de doeleinden van de gegevensverwerking van de nationale cyberbeveiligingscertificeringsautoriteit en van de in artikel 5, § 2 van het ontwerp bedoelde autoriteiten, in overeenstemming met overweging 55;

12. Verduidelijking van de kwalificatie van de verwerkingsverantwoordelijke, in overeenstemming met de overwegingen 56 en 57;

13. Schrapping van artikel 36, § 2 van het ontwerp (overw. 58 tot 64);

14. Exhaustieve precisering van de categorieën gegevens die de nationale cyberbeveiligingscertificeringsautoriteit en de in overeenstemming met artikel 5, § 2 aangewezen autoriteiten zullen verwerken bij de uitoefening van de opdrachten die hun door het voorontwerp van wet worden toevertrouwd in overeenstemming met de overwegingen 61 e.v.;

15. Aanpassing van de categorieën van betrokkenen ten aanzien van wie de in artikel 5 bedoelde autoriteiten gegevens zullen verwerken, in overeenstemming met de overwegingen 66 en 67;

16. Verduidelijking van artikel 39 van het ontwerp over de duur van de gegevensbewaring, in overeenstemming met overweging 69;

17. Beperking van de rechten van de betrokkenen uit hoofde van de AVG waarvan wordt afgeweken tot louter de rechten waarvan de uitoefening de inspectietaken in het gedrang brengt, en het bieden van een passend kader voor dergelijke afwijkingen van deze rechten en van de verplichting uit hoofde van artikel 20 van de WVP om een protocol voor gegevensuitwisseling te sluiten, in overeenstemming met de overwegingen 73 tot 81.

Imprimerie centrale – Centrale drukkerij