DOC 54 **0416/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

BUITENGEWONE ZITTING 2014

7 oktober 2014

WETSVOORSTEL

tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens wat de administratieve sancties, melding van lekken van gegevens, inzagerecht en informatieveiligheidsconsulenten betreft

(ingediend door de dames Sonja Becq en Nahima Lanjri en de heer Roel Deseyn)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

SESSION EXTRAORDINAIRE 2014

7 octobre 2014

PROPOSITION DE LOI

modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information

(déposée par Mmes Sonja Becq et Nahima Lanjri et M. Roel Deseyn)

SAMENVATTING

De indieners wensen het toezicht op de naleving van de privacywet te versterken, de administratieve rompslomp te verminderen, het inzagerecht in de eigen persoonsgegevens uit te breiden en een meldplicht bij datalekken in te voeren.

RÉSUMÉ

Les auteurs souhaitent renforcer le contrôle du respect de la loi relative à la protection de la vie privée, réduire les tracasseries administratives, élargir le droit de consultation des données à caractère personnel et instaurer une obligation de notification en cas de fuites de données.

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
FDF	:	*Fédéralistes Démocrates Francophones*
PP	:	*Parti Populaire*

Afkortingen bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*	*DOC 54 0000/000:*	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Schriftelijke Vragen en Antwoorden*	*QRVA:*	*Questions et Réponses écrites*
CRIV:	*Voorlopige versie van het Integraal Verslag*	*CRIV:*	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Beknopt Verslag*	*CRABV:*	*Compte Rendu Analytique*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*	*CRIV:*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Plenum*	*PLEN:*	*Séance plénière*
COM:	*Commissievergadering*	*COM:*	*Réunion de commission*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT:*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

TOELICHTING

DAMES EN HEREN,

Dit voorstel neemt de tekst over van voorstel DOC 53 1509/001.

Inleiding

Wetgeving is maar zo sterk als de controle op de naleving ervan. Dit geldt ook voor de bescherming van de privacy bij verwerking van persoonsgegevens. In België is er in tegenstelling tot onze buurlanden nog altijd geen privacywaakhond die snel kan optreden bij onachtzaam gebruik van persoonsgegevens. De privacycommissie beschikt niet over de mogelijkheid om administratieve boetes uit te schrijven bij grove schendingen van de privacywet.

Artsen, recruteerders, supermarkten, telecomoperatoren, websites, zoekmachines, direct marketeers, … allen verwerken ze intussen gegevens die vertellen wie we zijn, wat we doen, met wie we contact houden en waar we ons begeven. Bijna iedere nieuwe technologie en dienst genereert een nieuwe bron van elektronische persoonsgegevens: gsm, digitale tv, rfid-chips, … Meer dan ooit is correct omgaan met persoonsgegevens essentieel voor een vrije bewegingsruimte, een stabiele en democratische samenleving en een gezonde marktwerking. Privacy is niet alleen een individueel recht, de belangen die het tracht te verdedigen zijn ook collectief: autonomie en gelijke behandeling.

HOOFDSTUK 2

Inzagerecht — recht op dataoverdraagbaarheid

Een noodzakelijke voorwaarde om individuen een hoog niveau van gegevensbescherming te kunnen bieden is, dat de betrokkenen daadwerkelijk zeggenschap behouden over de gegevens die over hen worden bijgehouden. Toegang tot de verzamelde gegevens is terecht opgenomen in de Europese grondwet[1]. Het inzagerecht vindt zijn oorsprong in het verdrag nr. 108 van 28 januari 1981 van de Raad van Europa m.b.t. de

[1] Handvest van de grondrechten van de Europese Unie, art. 8, lid 2, 2000/C 364/01.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition reprend, en l'adaptant, le texte de la proposition DOC 53 1509/001.

Introduction

La force d'une législation dépend du contrôle de son respect. Cette règle vaut également pour la protection de la vie privée en cas de traitement de données à caractère personnel. En Belgique, contrairement à nos pays voisins, la législation relative à la vie privée n'a toujours pas de 'chien de garde' qui puisse intervenir rapidement en cas d'utilisation inappropriée de données à caractère personnel. La Commission de la protection de la vie privée n'a pas la possibilité d'infliger des amendes administratives en cas de violations graves de la loi relative à la protection de la vie privée.

Les médecins, recruteurs, supermarchés, opérateurs de télécommunications, sites internet, moteurs de recherche, responsables du marketing direct, … tous traitent des données qui révèlent qui nous sommes, ce que nous faisons, avec qui nous sommes en contact et où nous nous rendons. Presque chaque nouvelle technologie et chaque nouveau service génèrent une nouvelle source de données à caractère personnel électroniques: GSM, télévision numérique, puces RFID, … Plus que jamais, l'utilisation correcte des données à caractère personnel est essentielle pour garantir la liberté de mouvement, une société stable et démocratique et un fonctionnement sain du marché. La protection de la vie privée est non seulement un droit individuel, mais les intérêts qu'elle tente de défendre sont également collectifs: autonomie et égalité de traitement.

CHAPITRE 2

Droit de consultation — droit à la portabilité des données

Afin de garantir aux individus un niveau élevé de protection des données à caractère personnel, il est indispensable qu'ils gardent réellement la maîtrise des données qui sont conservées à leur sujet. L'accès aux données récoltées est, à juste titre, inscrit dans la constitution européenne[1]. Le droit de consultation trouve son origine dans la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à

[1] Charte des droits fondamentaux de l'Union européenne, art. 8, alinéa 2, 2000/C 364/01.

bescherming van personen bij de automatische verwerking van persoonsgegevens en werd uitgewerkt in de privacyrichtlijn 95/46/EG. Het is de verantwoordelijkheid vande Lidstaten aan te geven hoe deze informatie aan de betrokkenen wordt verstrekt[2].

Iedere burger heeft recht op een elektronische kopie van zijn persoonsgegevens: de voorgestelde wijziging creëert een recht op dataoverdraagbaarheid (*right of data portability*).

Het inzagerecht zoals bepaald in artikel 10 van de privacywet en het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens geeft elke persoon wiens gegevens worden verwerkt, het recht om van die gegevens mededeling te krijgen. De privacywet voorziet in uitzonderingen voor gegevens van politiediensten,... De verantwoordelijke voor verwerking dient deze gegevens, in begrijpelijke vorm, ten laatste binnen 45 dagen aan de betrokkene mee te delen.

De persoonsgegevens meedelen in een begrijpelijke vorm zoals de privacywet voorschrijft, wordt thans niet steeds geïnterpreteerd als een kopie van deze gegevens bezorgen in een bruikbare, elektronische vorm.

België kwam in 1992 met een aangepaste privacywetgeving voor geautomatiseerde verwerkingen. Het aantal geautomatiseerde verwerkingen en hun impact is sinds 1992 sterk toegenomen. Meester zijn van de eigen persoonsgegevens is meer dan ooit een noodzaak. Onder impuls van breedband internet en web 2.0 diensten worden steeds meer gegevens opgeladen, verwerkt en gestockeerd op het internet zelf. Er ontstonden *in the cloud* webdiensten voor het verwerken van teksten, foto's, boekhoudingen, bladwijzers, contactgegevens, ... Iedere burger moet vrij kunnen kiezen zijn gegevens te downloaden: wanneer hij een back-up wenst van zijn gegevens, deze nader wil bestuderen, wenst te veranderen van dienstenaanbieder, ... Transparantie bevordert het vertrouwen van de consument in nieuwe technologieën. Dataoverdraagbaarheid stimuleert een innovatieve en concurrentiële markt.

[2] Gewijzigd voorstel voor een richtlijn van de Raad betreffende de bescherming van natuurlijke personen in verband met de behandeling van persoonsgegevens en betreffende het vrije verkeer van die gegevens (door de Commissie krachtens artikel 149, lid 3,van het-EEG-Verdrag ingediend), COM(92) 422 def. - SYN 287, art 13.

l'égard du traitement automatisé des données à caractère personnel et il a été développé dans la directive 95/46/CE sur la protection de la vie privée. Il relève de la responsabilité des États membres d'indiquer comment ces informations sont communiquées aux personnes concernées[2].

Tout citoyen a le droit de recevoir une copie électronique de ses données à caractère personnel: la modification proposée crée un droit à la portabilité des données (*Right of Data Portability*).

Le droit de consultation tel qu'il est défini à l'article 10 de la loi sur la protection de la vie privée et dans l'arrêté royal du 13 février 2001 portant exécution 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 donne à toute personne dont les données sont traitées le droit d'obtenir communication de ces données. La loi sur la protection de la vie privée prévoit des exceptions pour les données des services de police,… Le responsable du traitement doit communiquer, sous une forme intelligible, ces données à la personne concernée dans un délai maximum de 45 jours.

L'obligation de communiquer les données à caractère personnel sous une forme intelligible, prévue dans la loi sur la protection de la vie privée, n'est actuellement pas toujours interprétée comme étant l'obligation de fournir une copie de ces données sous une forme électronique utilisable.

En 1992, la Belgique a adapté sa législation relative à la protection de la vie privée en vue de prendre en compte les traitements automatisés. Le nombre de traitements automatisés et leur impact ont fortement augmenté depuis 1992. Maîtriser ses propres données à caractère personnel est plus que jamais une nécessité. Sous l'impulsion de l'internet à haut débit et des services web 2.0, de plus en plus de données sont chargées, traitées et stockées sur l'internet même. Des services web "dans les nuages" ont vu le jour pour le traitement de textes, de photos, de comptabilités, de signets, de coordonnées,… Tout citoyen doit pouvoir choisir en toute liberté de télécharger ses données: lorsqu'il souhaite réaliser un backup de ses données, les examiner plus en détail, changer de prestataire de services, … La transparence favorise la confiance du consommateur dans les nouvelles technologies. La portabilité des données stimule le caractère innovateur et concurrentiel du marché.

[2] Proposition modifiée de directive du Conseil relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à la libre circulation des données (déposée par la Commission conformément à l'article 149, alinéa 3,du Traité CEE), COM(92) 422 def. - SYN 287, art 13.

HOOFDSTUK 3

Informatieveiligheidsconsulent

Wie in België persoonsgegevens wil verwerken — al dan niet met behulp van een computer — moet de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) daarvan op de hoogte brengen. Zowel bij de aanvang van de verwerking als bij wijziging dient men een aangifte te doen en een bijdrage te betalen: 25 euro voor een aangifte van een nieuwe verwerking via internet, 125 euro bij een papieren aangifte en 20 euro bij wijziging van de verwerking. De inkomsten voor de CBPL worden geraamd op 40 000 euro in 2009.

In de praktijk blijken heel wat personen en ondernemingen deze aangifteplicht niet na te leven. In 2008 waren er in totaal 4 133 aangiften bij de CBPL, waarvan 3 681 voor nieuwe verwerkingen[3]. Vermoed kan worden dat het aantal reële verwerkingen een veelvoud bedraagt. De aandacht voor de privacy bij de aanvang van de verwerking beperkt zich veelal tot een formaliteit. Hiermee gaat men voorbij aan de bedoelingen van de wetgever.

De eerste doelstelling van de wetgever was niet het creëren van extra administratieve formaliteiten maar de betrokkenen bewust maken van de privacyaspecten en mogelijke gevolgen. In de feiten blijkt dat het educatieve en sensibiliserende effect van deze formaliteiten bij de betrokkenen zeer beperkt is.

Een tweede doelstelling van de wetgever was om iedere Belg toe te laten om de informatie over de verwerking van zijn persoonsgegevens te bekomen via deze centrale aangiftenbank. Een register dat bijhield wie waar persoonsgegevens verwerkte. Geautomatiseerde verwerking gebeurde toen door een beperkt aantal, grote *mainframe* machines. Intussen heeft de ICT een enorme vlucht genomen.

Heeft een burger anno 2010 nood aan een centrale databank met formulieren om zijn vermoeden bevestigd te zien dat de arts, politicus, school of website die hij bezocht, persoonsgegevens verwerkt? In de praktijk zijn er nauwelijks mensen die deze weinig relevante informatie opvragen. Belangrijker voor deze burger is te weten welke gegevens over hem of haar werden opgeslagen (inzagerecht) en of dit gebeurde volgens de regels van de kunst.

[3] CBPL, Jaarverslag 2008, blz. 79.

CHAPITRE 3

Conseiller en sécurité de l'information

Quiconque souhaite traiter des données à caractère personnel en Belgique — à l'aide ou non d'un ordinateur — doit en informer la Commission de la protection de la vie privée (CPVP). Tant en début de traitement qu'en cas de modification de celui-ci, il faut faire une déclaration et payer une contribution: 25 euros pour une déclaration de nouveau traitement via internet, 125 euros pour une déclaration sur papier et 20 euros pour une modification du traitement. Les recettes pour la CPVP sont estimées à 40 000 euros en 2009.

Dans la pratique, il s'avère que de nombreuses personnes et entreprises ne respectent pas cette obligation de déclaration. En 2008, la CPVP a enregistré au total 4 133 déclarations, dont 3 681 pour de nouveaux traitements[3]. On peut supposer que le nombre de traitements réels est largement supérieur. L'attention portée à la protection de la vie privée en début de traitement se limite souvent à une formalité. On méconnaît ainsi les objectifs du législateur.

Le premier objectif du législateur était non pas de créer des formalités administratives supplémentaires, mais de sensibiliser les intéressés aux aspects liés à la protection de la vie privée et aux conséquences possibles. Dans les faits, il s'avère que l'effet éducatif et sensibilisateur de ces formalités est très limité chez les intéressés.

Une deuxième objectif du législateur consistait à permettre à chaque Belge d'obtenir, par l'intermédiaire de cette banque de déclarations centrale, des informations sur le traitement de ses données à caractère personnel, grâce à un registre renseignant qui traitait les données à caractère personnel et où il le faisait. À l'époque, un nombre limité de grosses machines "*mainframe*" effectuaient un traitement automatisé. Depuis lors, les TIC ont connu un essor considérable.

En 2010, un citoyen a-t-il besoin d'une banque de données centrale et de formulaires pour voir confirmer ses présomptions que le médecin, le responsable politique, l'école ou le site Internet qu'il a visité traite des données à caractère personnel? Dans la pratique, il y a très peu de personnes qui réclament ces informations peu pertinentes. Il est plus important pour ce citoyen de savoir quelles données le concernant ont été stockées (droit de consultation) et si cela s'est fait dans les règles de l'art.

[3] CPVP, Rapport annuel 2008, p. 79.

De Europese richtlijn laat toe om af te zien van de aangifteplicht, op voorwaarde dat men een specialist aanstelt die de privacyaspecten bewaakt, een zogenaamde *Data Protection Official*. Dit blijkt in bijvoorbeeld Duitsland[4] en Nederland[5] te zorgen voor een bewustzijn rond privacy, een dynamiek van kennisuitwisseling, toegepaste opleidingen[6], netwerken[7] van specialisten in nauw contact met de nationale privacycommissie. Binnen de eigen organisatie genieten ze grote autonomie en leggen ze zich toe op controle vooraf, advies, opleiding, interne audit met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Dit alternatief voor de aangifteplicht is momenteel in vijf EU-landen geïmplementeerd[8]: Duitsland[9], Nederland[10], Zweden, Luxemburg en Frankrijk.

De huidige Belgische omzetting van de richtlijn voorziet in een verplichting tot aanmelding. Dit wetsvoorstel vervangt deze aangifteverplichting door de aanduiding van een privacyexpert (zogenaamde informatieveiligheidsconsulent). Wie werkt met persoonsgegevens is meer gediend met een concreet aanspreekpunt dan met een papier in de kast. Deze privacyexpert is binnen een organisatie de onafhankelijke toezichthouder op de toepassing van de privacywetgeving. Hij heeft als taak toe te zien op het veilig en correct omgaan met persoonsgegevens veeleer dan op het vervullen van administratieve formaliteiten. Het gaan niet om een bijkomend personeelslid, het staat de betrokken organisatie vrij aan deze persoon andere taken te geven. Deze rol van consulent kan opgenomen worden door een externe of interne medewerker. Organisaties die weinig of slechts sporadisch persoonsgegevens verwerken, worden naar analogie met het buitenland vrijgesteld van deze verplichting.

La directive européenne permet de renoncer à l'obligation de déclaration, pourvu que l'on désigne un spécialiste chargé de veiller aux aspects liés à la protection de la vie privée, un détaché à la protection des données. Il s'avère qu'en Allemagne[4] et aux Pays-Bas[5], par exemple, cette alternative donne lieu à une prise de conscience en matière de protection de la vie privée, à une dynamique d'échange de connaissances, à des formations appliquées[6], à la création des réseaux[7] de spécialistes entretenant des contacts étroits avec la commission nationale de protection de la vie privée. Au sein de leur propre organisation, ces spécialistes bénéficient d'une large autonomie et se focalisent sur le contrôle préalable, la formulation d'avis, la formation, l'audit interne en ce qui concerne le traitement automatisé de données à caractère personnel. Pour l'heure, cinq États membres de l'Union européenne appliquent cette alternative à l'obligation de déclaration[8]: l'Allemagne[9], les Pays-Bas[10], la Suède, le Luxembourg et la France.

La transposition actuelle de la directive en droit belge prévoit une obligation de déclaration. La présente proposition de loi remplace cette obligation de déclaration par la désignation d'un expert en protection de la vie privée (le "conseiller en sécurité de l'information"). Quiconque traite des données à caractère personnel gagnera davantage à disposer d'un point de contact concret que d'un papier dans une armoire. Au sein de l'organisation, cet expert en protection de la vie privée est le contrôleur indépendant de l'application de la législation relative à la protection de la vie privée. Sa tâche consiste plutôt à veiller à l'utilisation correcte et sûre des données à caractère personnel qu'à remplir des formalités administratives. Il ne s'agit pas d'un membre de personnel supplémentaire, l'organisation concernée ayant le loisir de confier d'autres tâches à cette personne. Ce rôle de conseiller peut être assumé par un collaborateur externe ou interne. À l'instar de ce qui se fait à l'étranger, les organisations qui traitent peu de données à caractère personnel ou qui n'en traitent que de manière sporadique sont exemptées de cette obligation.

4 *Die Datenschutzbeauftragten in Behörde und Betrieb. BfDI-Info 4. 8. Auflage. Mai 2010. http://www.bfdi.bund.de/cae/servlet/contentblob/416308/publicationFile/88786/INFO4.pdf*
5 De functionaris gegevensbescherming http://www.cbpweb.nl/downloads_brochures/bro_fg.pdf
6 Nederlandse beroepsvereniging van Functionarissen Gegevensbescherming http://www.ngfg.nl/producten_opleidingen.html
7 *Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) https://www.bvdnet.de/rgtreffen.html?&no_cache=1*
8 Article 29 Data Protection Working Party, 1021105/EN WP 106, Hfdst 5.
9 Bundesdatenschutzgesetz § 4f en § 4g.
10 Wet bescherming persoonsgegevens art. 64.

4 *Die Datenschutzbeauftragten in Behörde und Betrieb. BfDI-Info 4. 8. Auflage*. Mai 2010. http://www.bfdi.bund.de/cae/servlet/contentblob/416308/publicationFile/88786/INFO4.pdf
5 Le *functionaris gegevensbescherming* http://www.cbpweb.nl/downloads_brochures/bro_fg.pdf
6 Association professionnelle néerlandaise des fonctionnaires chargés de la protection des données http://www.ngfg.nl/producten_opleidingen.html
7 *Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) https://www.bvdnet.de/rgtreffen.html?&no_cache=1*
8 Groupe de travail "Article 29" sur la protection des données, 1021105/FR WP 106, Chapitre 5.
9 *Bundesdatenschutzgesetz*, § 4f en § 4g.
10 *Wet bescherming persoonsgegevens* art. 64.

HOOFDSTUK 4

Administratieve sancties

In theorie worden inbreuken op de naleving van de privacywet vervolgd. In de praktijk worden deze klachten geseponeerd. Bovendien kan, gelet op de kostprijs van ICT-beveiliging en op de marktwaarde van persoonlijke informatie, een kleine kans op een eventuele strafrechterlijke boete van 2 500 euro weinig afschrikwekkend genoemd worden.

Administratieve boetes door de toezichthoudende autoriteit bieden een uitweg. Het laat de privacyautoriteit toe snel te reageren op de snelle technologische evoluties. Het risico op een adminstratieve boete zal een effectieve sensibiliserende en corrigerende rol vervullen. In verschillende lidstaten (bijvoorbeeld Frankrijk, Spanje, …) hebben de toezichthoudende autoriteiten intussen een reële sanctiebevoegdheid.

Het opheffen van de aangifteplicht en het versterken van het toezicht zijn in lijn met de recente aanbevelingen van de zogenaamde werkgroep artikel 29[11] van de Europese privacyauthoriteiten. De privacywetgeving en de toezichtmogelijkheden van de CBPL blijven met dit wetsvoorstel onverminderd van toepassing bij iedere gegevensverwerking. Opgemerkt dient dat dit wetsvoorstel geen afbreuk doet aan de specifieke regeling van de plaatsing en het gebruik van bewakingscamera's (wet van 21 maart 2007).

HOOFDSTUK 5

Melden van lekken van gegevens

Baas zijn over de eigen gegevens betekent ook op de hoogte gebracht worden bij diefstal van deze gegevens. Wanneer persoonsgegevens zoals paswoorden, bankkaartgegevens, pincodes, … gehackt worden of in handen komen van derden dan weet de betrokkene dit graag snel. Bedrijven die gegevens verliezen, moeten daar over communiceren. Telkens de persoonlijke gegevens in gevaar zijn, zal de verantwoordelijke voor de verwerking openlijk moeten communiceren en de betrokkenen alsook de privacywaakhond inlichten. Dergelijke meldplicht zal een bijkomend drukkingsmiddel

[11] Article 29 Data Protection Working Party, "The Future of Privacy", 02356/09/EN WP 168, 1 december 2009, lemma 84, 86 & 90.

CHAPITRE 4

Sanctions administratives

En théorie, le non-respect de la loi relative à la protection de la vie privée est poursuivi mais, en pratique, les plaintes concernées sont classées sans suite. De plus, compte tenu du coût de la sécurisation TIC et de la valeur marchande des informations à caractère personnel, le faible risque d'une éventuelle amende pénale de 2 500 euros ne peut pas être qualifié de dissuasif.

Une solution consiste à permettre à l'autorité de contrôle d'infliger des amendes administratives. Cette solution permettrait à l'autorité précitée de réagir avec célérité aux évolutions technologiques rapides. Le risque de se voir infliger une amende administrative jouera un rôle effectif de sensibilisation et de correction. Dans plusieurs États membres (par exemple en France, en Espagne, *etc*.), les autorités de contrôle ont déjà de réelles compétences de sanction.

La suppression de l'obligation de déclaration et le renforcement du contrôle se situent dans le prolongement des recommandations récentes du Groupe de travail "Article 29"[11] sur la protection des données des autorités européennes. La présente proposition de loi ne porte aucunement préjudice à l'application de la législation sur la vie privée, ni des compétences de contrôle de la CPVP lors de chaque traitement de données. La présente proposition de loi ne porte en outre aucun préjudice à la réglementation spécifique sur l'installation et l'utilisation de caméras de surveillance (loi du 21 mars 2007).

CHAPITRE 5

Notification des fuites de données

Pour être maître de ses propres données, il faut également être informé de leur vol. Les personnes dont les données personnelles (mots de passe, données de cartes bancaires, codes PIN, *etc*.) sont piratées ou transmises à des tiers aiment en être informées rapidement. Les entreprises qui perdent ces données doivent le signaler. Chaque fois que des données à caractère personnel sont menacées, le responsable du traitement devra le signaler publiquement et en informer les intéressés et les autorités chargées de la protection de la vie privée. Cette obligation de notification sera un moyen

[11] Groupe de travail "Article 29" sur la protection des données, "L'avenir de la protection de la vie privée", 02356/09/FR WP 168, 1er décembre 2009, points 84, 86 & 90.

worden. Organisaties zullen erdoor meer gaan letten op de persoonlijke gegevens waarover ze beschikken en op de noodzaak tot beveiliging.

In 2009 voerde de zogenaamde Telecom Package[12] reeds deze meldplicht in voor telecomoperatoren en wijzigde daartoe e-privacyrichtlijn[13].

Een algemene meldplicht van datalekken is reeds in voege in Duitsland[14] (2009), Oostenrijk[15] (2010), Canada, Australia[16] en in bijna alle staten in de VS.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK 1

Algemene bepaling

Artikel 1

Optioneel bicamerale procedure (artikel 78 van de Grondwet).

HOOFDSTUK 2

Inzagerecht

Art. 2

Verduidelijking dat het inzagerecht in geval van geautomatiseerde verwerking, recht geeft op mededeling van deze gegevens in een begrijpbare, bruikbare, gebruiksvriendelijke, elektronische vorm.

De mogelijkheid om inzage te krijgen van de gegevens op een niet digitale wijze, indien de betrokkene dit wenst, blijft behouden.

[12] Richtlijn van 2009/136/EG, art. 2.
[13] Richtlijn 2002/58/EG, artikelen 4.3 en 4.4, tweede lid nieuw.
[14] *Bundesdatenschutzgesetz § 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.*
[15] *Bundesgesetz über den Schutz personenbezogener Daten § 24 (2a).*
[16] *Data Breach Notification Law Across the World from California to Australia, Alana Maurushat, University of New South Wales, 2009.*

de pression supplémentaire. Les organisations seront dès lors plus attentives aux données personnelles dont elles disposent et à la nécessité de les sécuriser.

En 2009, le paquet "Telecom"[12] a déjà prévu cette obligation de notification pour les opérateurs de télécommunications et modifié, à cette fin, la directive concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques[13].

Une obligation générale de notification des fuites de données est déjà en vigueur en Allemagne[14] (2009), en Autricle[15] (2010), au Canada, en Australie[16] et dans presque tous les états des États-Unis.

COMMENTAIRE DES ARTICLES

CHAPITRE 1ER

Dispositif général

Article 1er

Procédure bicamérale optionnelle (article 78 de la Constitution).

CHAPITRE 2

Droit de consultation

Art. 2

Il est précisé que le droit de consultation donne lieu, en cas de traitement automatisé, à la communication de ces données sous une forme électronique compréhensible, efficace et conviviale.

La possibilité d'accéder aux données de manière non numérique, si la personne concernée le souhaite, est maintenue.

[12] Directive 2009/136/CE, art. 2.
[13] Directive 2002/58/CE, articles 4.3 et 4.4, nouveau paragraphe 2.
[14] *Bundesdatenschutzgesetz § 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.*
[15] *Bundesgesetz über den Schutz personenbezogener Daten § 24 (2a).*
[16] *Data Breach Notification Law Across the World from California to Australia, Alana Maurushat, University of New South Wales, 2009.*

HOOFDSTUK 3

Informatieveiligheidsconsulent

Art. 3 tot 10

De aangifteplicht wordt opgeheven. De verantwoordelijke voor verwerking dient voortaan een informatieveiligheidsconsulent aan te duiden. De informatieveiligheidsconsulent heeft een adviserende, stimulerende, documenterende en controlerende opdracht. Niet-publieke organisaties die weinig of sporadisch persoonsgegevens verwerken, worden vrijgesteld van deze verplichting. De betrokken organisatie heeft de keuzevrijheid om een eigen medewerker dan wel externe consultant aan te wijzen voor deze rol.

Art. 11

Het CBPL behoudt de mogelijkheid om alle inlichtingen die tot nu toe via de aangifte werden verstrekt, op te vragen.

HOOFDSTUK 4

Administratieve sancties

Art. 12

Het CBPL wordt verzocht jaarlijks uitvoerig te rapporteren over het gevoerde administratieve sanctiebeleid.

Art. 13

Het CBPL wordt gemachtigd administratief op te treden bij inbreuken.

CHAPITRE 3

Conseiller en sécurité de l'information

Art. 3 à 10

L'obligation de déclaration est supprimée. Le responsable du traitement doit désigner dorénavant un conseiller en sécurité de l'information. Celui-ci est chargé de conseiller, d'encourager, de documenter et de contrôler. Les organisations non publiques qui traitent peu ou sporadiquement des données à caractère personnel sont dispensées de cette obligation. L'organisation concernée est libre de désigner un de ses collaborateurs ou un conseiller externe pour accomplir cette mission.

Art. 11

La CPVP conserve la possibilité de demander toutes les informations qui ont été communiquées jusqu'à ce jour par le biais de la déclaration.

CHAPITRE 4

Sanctions administratives

Art. 12

La CPVP est chargée d'établir un rapport annuel détaillé sur la politique menée en matière de sanctions administratives.

Art. 13

La CPVP est habilitée à prendre des mesures administratives en cas d'infractions.

HOOFDSTUK 5

Melden van lekken van gegevens

Art. 14

Wanneer gevoelige persoonsgegevens met betrekking tot gezondheid, politieke voorkeur, seksueel leven, religie, vervolgingen of veroordelingen alsook authentificatiegegevens (paswoorden) en gegevens die vallen onder beroepsgeheim gestolen worden en er ernstige schade dreigt voor de betrokkenen, dient de CBPL alsook de betrokkene onverwijld ingelicht te worden.

Sonja BECQ (CD&V)
Nahima LANJRI (CD&V)
Roel DESEYN (CD&V)

CHAPITRE 5

Notification de fuites de données

Art. 14

Lorsque des données sensibles à caractère personnel relatives à la santé, aux préférences politiques, à la vie sexuelle, à la religion, aux poursuites ou aux condamnations, ainsi que des données d'authentification (mots de passe) et des données relevant du secret professionnel sont volées et que les intéressés risquent de subir un préjudice grave, la CPVP et l'intéressé doivent en être immédiatement informés.

WETSVOORSTEL

HOOFDSTUK 1

Algemene bepaling

Artikel 1

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

HOOFDSTUK 2

Inzagerecht

Art. 2

In artikel 10 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, vervangen bij de wet van 11 december 1998 en gewijzigd bij de wet van 22 augustus 2002, worden in § 1 de volgende wijzigingen aangebracht:

1° het derde lid wordt aangevuld met de volgende zin: “In geval van geautomatiseerde verwerking kan de betrokkene verzoeken de inlichtingen die elektronisch zijn opgeslagen, elektronisch mede te delen.”;

2° het vierde lid, wordt aangevuld met de woorden: “in bijzonder wat de authentificatie van de betrokkene betreft.”

HOOFDSTUK 3

Informatieveiligheidsconsulent

Art. 3

In artikel 3 van dezelfde wet, laatstelijk gewijzigd bij de wet van 17 juni 2013, worden de volgende wijzigingen aangebracht:

1° in § 3, d) worden de woorden “17, § 3, 9° en 12°, § 4 en § 8, evenals de artikelen 18, 21 en 22” vervangen door de woorden “17 en 19, § 2, 7° en 10° en § 3, evenals de artikelen 21 en 22”;

2° in § 4 worden de woorden “17*bis*, eerste lid, 18, 20” opgeheven.

PROPOSITION DE LOI

CHAPITRE 1er

Disposition générale

Article 1er

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

CHAPITRE 2

Droit de consultation

Art. 2

Dans l’article 10 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, remplacé par la loi du 11 décembre 1998 et modifié par la loi du 22 août 2002, dans le § 1er, les modifications suivantes sont apportées:

1° l’alinéa 3 est complété par la phrase suivante: “En cas de traitement automatisé, la personne concernée peut demander la communication par la voie électronique des renseignements archivés électroniquement.”;

2° l’alinéa 4 est complété par les mots: “, en particulier en ce qui concerne l’authentification de la personne concernée.”

CHAPITRE 3

Conseiller en sécurité de l’information

Art. 3

Dans l’article 3 de la même loi, modifié en dernier lieu par la loi du 17 juin 2013, les modifications suivantes sont apportées:

1° dans le § 3, d), les mots “17, § 3, 9° et 12°, § 4 et § 8, ainsi que les articles 18, 21 et 22” sont remplacés par les mots “17 et 19, § 2, 7° et 10°, et § 3, ainsi que les articles 21 et 22”;

2° dans le § 4, les mots “, 17*bis*, alinéa 1er, 18, 20” sont abrogés.

Art. 4

In artikel 10 van dezelfde wet, vervangen bij de wet van 11 december 1998 en gewijzigd bij de wet van 22 augustus 2002, worden in § 1 in de bepaling onder d) de woorden “en eventueel inzage te nemen van het in artikel 18 bedoelde openbaar register” opgeheven.

Art. 5

In artikel 16, § 2 van dezelfde wet, vervangen bij de wet van 11 december 1998, wordt de bepaling onder 4° opgeheven.

Art. 6

Artikel 17 van dezelfde wet wordt vervangen als volgt:

“Art. 17. § 1. De verantwoordelijke voor de verwerking wijst, alleen of samen met andere verantwoordelijken, een informatieveiligheidsconsulent aan. Deze verplichting geldt niet voor natuurlijke personen en private rechtspersonen die hoogstens negen personen voortdurend tewerkstellen voor het geautomatiseerd verwerken van persoonsgegevens.

§ 2. Als informatieveiligheidsconsulent kan slechts worden benoemd een natuurlijke persoon die voor de vervulling van zijn taak over voldoende kennis beschikt en voldoende betrouwbaar kan worden geacht.

De informatieveiligheidsconsulent kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd.

Hij ondervindt geen nadeel van de uitoefening van zijn taak en wordt door de verantwoordelijke in de gelegenheid gesteld zijn taak naar behoren te vervullen.

Hij is verplicht tot geheimhouding van hetgeen hem op grond van een klacht of een verzoek van betrokkene is bekend geworden, tenzij de betrokkene in bekendmaking toestemt.

§ 3. De informatieveiligheidsconsulent ziet toe op de naleving van de privacywetgeving, op het risicobeheer, op het voorkomen en het vlug en doeltreffend herstellen van schade aan persoonsgegevens en op het voorkomen van onrechtmatige schendingen van de persoonlijke levenssfeer van de betrokkenen.

Art. 4

Dans l’article 10 de la même loi, remplacé par la loi du 11 décembre 1998 et modifié par la loi du 22 août 2002, dans le § 1er, d), les mots “et, éventuellement, de consulter le registre public prévu à l’article 18” sont abrogés.

Art. 5

Dans l’article 16, § 2, de la même loi, remplacé par la loi du 11 décembre 1998, le 4° est abrogé.

Art. 6

L’article 17 de la même loi est remplacé par ce qui suit:

“Art. 17. § 1er. Le responsable du traitement désigne, seul ou avec d’autres responsables, un conseiller en sécurité de l’information. Cette obligation ne s’applique pas aux personnes physiques et aux personnes morales privées qui n’occupent en permanence pas plus de neuf personnes pour le traitement automatisé de données à caractère personnel.

§ 2. Ne peut être désignée comme conseiller en sécurité de l’information qu’une personne physique qui dispose d’une connaissance suffisante pour accomplir sa tâche et qui peut être considérée comme suffisamment fiable.

Le conseiller en sécurité de l’information ne peut, en ce qui concerne l’exercice de sa fonction, recevoir aucune instruction du responsable ou de l’organisation qui l’a nommé.

Il ne subit aucun préjudice en raison de l’exercice de sa fonction et le responsable lui donne la possibilité de remplir correctement sa tâche.

Il est tenu de respecter la confidentialité des informations dont il a eu connaissance à la suite d’une plainte ou d’une demande de l’intéressé, sauf si celui-ci en autorise la publication.

§ 3. Le conseiller en sécurité de l’information veille au respect de la législation sur la protection de la vie privée, à la gestion des risques, à la prévention et à la réparation rapide et efficiente des dommages aux données à caractère personnel et des violations illégitimes de la vie privée des intéressés.

§ 4. De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de taken en het statuut van de informatieveiligheidsconsulent."

Art. 7

Artikel 17*bis* van dezelfde wet, ingevoegd bij de wet van 11 december 1998, wordt opgeheven.

Art. 8

Artikel 18 van dezelfde wet, gewijzigd bij de wet van 11 december 1998, wordt opgeheven.

Art. 9

Artikel 19 van dezelfde wet, gewijzigd bij de wet van 11 december 1998, wordt vervangen als volgt:

§ 1. Wanneer de Commissie voor de bescherming van de persoonlijke levenssfeer meent dat een verwerking van persoonsgegevens een mogelijke schending van de persoonlijke levenssfeer inhoudt, kan zij hetzij ambtshalve, hetzij op verzoek van een betrokkene de verantwoordelijke voor de verwerking opleggen haar het geheel of een gedeelte van de inlichtingen opgesomd in § 2 mede te delen.

§ 2. Volgende inlichtingen worden verstrekt:

1° de naam, de voornamen en het volledig adres of de benaming en de zetel van de verantwoordelijke voor de verwerking en in voorkomend geval van zijn vertegenwoordiger in België;

2° de benaming van de verwerking;

3° het doel of het geheel van samenhangende doeleinden van de geautomatiseerde verwerking;

4° de categorieën van de verwerkte persoonsgegevens met een bijzondere beschrijving van de gegevens bedoeld in de artikelen 6 tot 8;

5° de categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;

6° de waarborgen die aan de mededeling van gegevens aan derden verbonden moeten zijn;

§ 4. Le Roi fixe, par arrêté délibéré en Conseil des ministres et après avis de la Commission de la protection de la vie privée, les missions et le statut du conseiller en sécurité de l'information."

Art. 7

L'article 17*bis* de la même loi, inséré par la loi du 11 décembre 1998, est abrogé.

Art. 8

L'article 18 de la même loi, inséré par la loi du 11 décembre 1998, est abrogé.

Art. 9

L'article 19 de la même loi, inséré par la loi du 11 décembre 1998, est remplacé par ce qui suit:

§ 1er. Lorsque la Commission de la protection de la vie privée estime qu'un traitement de données à caractère personnel est susceptible de por*ter* atteinte à la vie privée, elle peut soit d'office, soit sur requête d'une personne concernée enjoindre au responsable du traitement de lui communiquer tout ou partie des informations énumérées au § 2.

§ 2. Les informations suivantes sont fournies:

1° les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et, le cas échéant, de son représentant en Belgique;

2° la dénomination du traitement;

3° la finalité ou l'ensemble des finalités liées du traitement automatisé;

4° les catégories de données à caractère personnel qui sont traitées avec une description particulière des données visées aux articles 6 à 8;

5° les catégories de destinataires à qui les données peuvent être fournies;

6° les garanties dont doit être entourée la communication de données aux tiers;

7° de wijze waarop de personen op wie de gegevens betrekking hebben daarvan in kennis worden gesteld, de dienst waarbij het recht op toegang kan worden uitgeoefend en de maatregelen genomen om de uitoefening van dat recht te vergemakkelijken;

8° de termijn waarna, in voorkomend geval, de gegevens niet meer mogen bewaard, gebruikt of verspreid worden;

9° een algemene beschrijving om op voorhand te kunnen beoordelen of de veiligheidsmaatregelen die in toepassing van artikel 16 van deze wet genomen zijn, afdoende zijn;

10° de redenen waarop de verantwoordelijke voor de verwerking in voorkomend geval de toepassing van artikel 3, § 3, van deze wet steunt;

11° wanneer de verwerkte gegevens, zelfs occasioneel, bestemd zijn om naar het buitenland te worden doorgezonden, voor elke categorie van gegevens, het land van bestemming.

§ 3. In het kader van haar controle- en onderzoeksbevoegdheid bedoeld in artikel 31 en 32 is de Commissie voor de bescherming van de persoonlijke levenssfeer gemachtigd tot het opeisen van andere gegevens, met name de oorsprong van de persoonsgegevens, de gekozen automatiseringstechniek en de voorziene beveiligingsmaatregelen."

Art. 10

Artikel 20 van dezelfde wet wordt opgeheven.

Art. 11

In artikel 39 van dezelfde wet, laatstelijk gewijzigd bij de wet van 26 juni 2000, worden de volgende wijzigingen aangebracht:

a) de bepaling onder 7° wordt vervangen als volgt: "7° de verantwoordelijke voor de verwerking, zijn vertegenwoordiger in België, zijn aangestelde of gemachtigde die, in overtreding van artikel 19, weigert om aan de Commissie de informatie mee te delen of onvolledige of onjuiste inlichtingen verstrekt;"

b) de bepalingen onder 8° en 10° worden opgeheven.

7° les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit;

8° la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées;

9° une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises en application de l'article 16 de la présente loi;

10° les motifs sur lesquels le responsable du traitement fonde, le cas échéant, l'application de l'article 3, § 3, de la présente loi;

11° si les données traitées sont destinées, même occasionnellement, à faire l'objet d'une transmission vers l'étranger, pour chaque catégorie de données, le pays de destination.

§ 3. Dans le cadre de ses pouvoirs de contrôle et d'enquête prévus à l'article 31 et 32, la Commission de la protection de la vie privée a le pouvoir d'exiger d'autres éléments d'information, notamment l'origine des données à caractère personnel, la technique d'automatisation choisie et les mesures de sécurité prévues."

Art. 10

L'article 20 de la même loi est abrogé.

Art. 11

Dans l'article 39 de la même loi, modifié en dernier lieu par la loi du 26 juin 2000, les modifications suivantes sont apportées:

a) le 7° est remplacé par ce qui suit: "7° le responsable du traitement, son représentant en Belgique, son préposé ou mandataire qui, en violation de l'article 19, refuse de communiquer des informations à la Commission ou lui fournit des informations incomplètes ou inexactes;"

b) le 8° et le 10° sont abrogés.

HOOFDSTUK 4

Administratieve sancties

Art. 12

In artikel 32, § 2, van dezelfde wet, gewijzigd bij de wet van 11 december 1998, worden de woorden “en 18” vervangen door de woorden “, 19, 32 en 39/2”.

Art. 13

In dezelfde wet wordt een artikel 39/2 ingevoegd, luidende:

“Art. 39/2. § 1. De Commissie voor de bescherming van de persoonlijke levenssfeer deelt, in geval van een overtreding op de wetgeving of reglementering waarvan de naleving door de Commissie voor de bescherming van de persoonlijke levenssfeer wordt gecontroleerd, zijn grieven mee aan de overtreder, alsook het beoogde bedrag van de administratieve boete die aan de schatkist toekomt ten bedrage van maximaal 10 000 euro. De hierboven vermelde geldboete kan worden verdubbeld in geval van een nieuwe overtreding op de hierboven vermelde wetgeving of regelgeving binnen drie jaar na de eerste veroordeling.

§ 2. De Commissie voor de bescherming van de persoonlijke levenssfeer stelt de termijn vast waarover de overtreder beschikt om het dossier te raadplegen en zijn schriftelijke opmerkingen voor te leggen. Deze termijn mag niet kor*ter* zijn dan vijftien werkdagen.

§ 3. De overtreder wordt uitgenodigd om te verschijnen op de datum die door de Commissie voor de bescherming van de persoonlijke levenssfeer bij aangetekende brief wordt meegedeeld. Hij mag zich laten vertegenwoordigen door de raadsman van zijn keuze.

§ 4. De Commissie voor de bescherming van de persoonlijke levenssfeer kan elke persoon horen die nuttige informatie kan verschaffen, hetzij ambtshalve, hetzij op verzoek van de overtreder.

§ 5. De Commissie voor de bescherming van de persoonlijke levenssfeer neemt een besluit binnen zestig dagen na de sluiting van de debatten.

Binnen vijf dagen wordt dit besluit per aangetekende brief aan de betrokkene meegedeeld en bekendgemaakt op de webstek van Commissie voor de bescherming van de persoonlijke levenssfeer.

CHAPITRE 4

Sanctions administratives

Art. 12

Dans l’article 32, § 2, de la même loi, modifié par la loi du 11 décembre 1998, les mots “et 18” sont remplacés par les mots “, 19, 32 et 39/2”.

Art. 13

Dans la même loi, il est inséré un article 39/2 rédigé comme suit:

“Art. 39/2. § 1er. En cas d’infraction à la législation ou à la réglementation dont elle contrôle le respect, la Commission de la protection de la vie privée notifie ses griefs au contrevenant ainsi que le montant envisagé de l’amende administrative au profit du Trésor public d’un montant maximal de 10 000 euros. L’amende précitée peut être doublée en cas de nouvelle infraction à la législation ou à la réglementation susmentionnées dans les trois ans qui suivent la première condamnation.

§ 2. La Commission de la protection de la vie privée fixe le délai dont dispose le contrevenant pour consulter le dossier et présenter ses observations écrites. Ce délai ne peut être inférieur à quinze jours ouvrables.

§ 3. Le contrevenant est invité à comparaître à la date fixée par la Commission de la protection de la vie privée et communiquée par lettre recommandée. Il peut se faire représenter par le conseil de son choix.

§ 4. La Commission de la protection de la vie privée peut entendre toute personne pouvant fournir des informations utiles, soit d’office, soit à la demande du contrevenant.

§ 5. La Commission de la protection de la vie privée rend une décision dans les soixante jours qui suivent la clôture des débats.

Dans les cinq jours, cette décision est notifiée à l’intéressé par lettre recommandée et publiée sur le site Internet de la Commission de la protection de la vie privée.

§ 6. De overtreder die de uitspraak betwist waarbij de Commissie voor de bescherming van de persoonlijke levenssfeer een geldboete oplegt, kan binnen een termijn van een maand te rekenen vanaf de kennisgeving van de uitspraak van de commissie door middel van een verzoekschrift beroep instellen bij de rechtbank van eerste aanleg van zijn woonplaats of maatschappelijke zetel."

HOOFDSTUK 5

Melding van lekken van gegevens

Art. 14

In dezelfde wet wordt een artikel 16/2 ingevoegd, luidende:

"Art. 16/2. § 1. Wanneer de verantwoordelijke voor de verwerking vaststelt dat bij hem verwerkte persoonsgegevens onrechtmatig doorgegeven zijn of dat derden op een andere wijze onrechtmatig kennis hebben genomen van bij hem verwerkte persoonsgegevens en er ernstige schade dreigt voor de betrokkenen, informeert hij de betrokkenen en de Commissie op de wijze omschreven in dit artikel.

§ 2. De inkennisstelling is vereist bij inbreuken in verband met volgende persoonsgegevens:

1° gevoelige persoonsgegevens bedoeld in art. 6, § 1; art. 7, § 1 en art. 8, § 1;

2° persoonsgegevens die onder een beroepsgeheim vallen;

3° persoonsgegevens gebruikt voor authenticatie.

§ 3. De kennisgeving aan de betrokkenen vermeldt ten minste:

1° de aard van de inbreuk in verband met persoonsgegevens;

2° de contactpunten voor meer informatie;

3° de aanbevolen maatregelen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten.

§ 6. Le contrevenant qui conteste la décision par laquelle la Commission de la protection de la vie privée inflige une amende peut interje*ter* appel par requête auprès du tribunal de première instance de son domicile ou de son siège social, dans un délai d'un mois à compter de la notification de la décision de la commission."

CHAPITRE 5

Notification des fuites de données

Art. 14

Dans la même loi, il est inséré un article 16/2 rédigé comme suit:

"Art. 16/2. § 1er. Lorsque le responsable du traitement constate que des données à caractère personnel qu'il a traitées ont été transmises indûment ou que des tiers en ont pris connaissance indûment d'une autre manière, et que les personnes concernées risquent de subir des dommages graves, il informe ces dernières et la Commission selon les modalités définies au présent article.

§ 2. La notification est requise en cas de violation concernant les données à caractère personnel suivantes:

1° données à caractère personnel sensibles visées aux articles 6, § 1er, 7, § 1er et 8, § 1er;

2° données à caractère personnel relevant du secret professionnel;

3° données à caractère personnel utilisées à des fins d'authentification.

§ 3. La notification faite aux personnes concernées mentionne au minimum:

1° la nature de la violation concernant des données à caractère personnel;

2° les points de contact auprès desquels des informations supplémentaires peuvent être obtenues;

3° les mesures préconisées pour atténuer les conséquences négatives possibles de la violation concernant des données à caractère personnel.

De kennisgeving aan de Commissie bevat bovendien een omschrijving van de gevolgen van de inbreuk en van de door de verantwoordelijke voor de verwerking voorgestelde of getroffen maatregelen om de inbreuk in verband met persoonsgegevens aan te pakken.

§ 4. De Commissie wordt onverwijld in kennis gesteld.

De betrokkenen worden in kennis gesteld zodra maatregelen genomen werden om de persoonsgegevens te beschermen of onverwijld wanneer deze maatregelen niet onmiddellijk genomen worden.

Inkennisstelling van de betrokkenen van een inbreuk in verband met persoonsgegevens is niet vereist wanneer de verantwoordelijke voor de verwerking tot voldoening van de Commissie heeft aangetoond dat hij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de gegevens die bij de beveiligingsinbreuk betrokken waren. Met technologische beschermingsmaatregelen worden die maatregelen bedoeld die de persoonsgegevens onbegrijpelijk maken voor eenieder die geen recht op toegang daartoe heeft en die ernstige schade als gevolg van eventueel misbruik van de persoonsgegevens voorkomen.

Onverminderd de verplichting van de verantwoordelijke voor de verwerking om de betrokkenen in kennis te stellen, kan de Commissie de verantwoordelijke voor de verwerking, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

De Koning kan na advies van de Commissie nadere regels bepalen met betrekking tot de inkennisstelling aan de betrokkenen en aan de Commissie.

§ 5. De verantwoordelijke voor de verwerking houdt een inventaris bij van inbreuken op persoonsgegevens, onder meer met de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, zodat de Commissie kan nagaan of de bepalingen van dit artikel worden nageleefd. De inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens."

La notification à la Commission décrit en outre les conséquences de la violation et les mesures proposées ou prises par le responsable du traitement pour y remédier.

§ 4. La Commission est informée sans délai.

Les personnes concernées sont informées dès que des mesures ont été prises pour protéger les données à caractère personnel ou sont informées sans retard si ces mesures ne sont pas prises sur-le-champ.

La notification aux personnes concernées d'une violation de données à caractère personnel n'est pas nécessaire si le responsable du traitement a prouvé, à la satisfaction de la Commission, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. Par mesures de protection technologiques, on entend les mesures qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès et qui permettent d'éviter un préjudice grave consécutif à une éventuelle utilisation abusive des données à caractère personnel.

Sans préjudice de l'obligation du responsable du traitement d'informer les personnes concernées, la Commission peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du responsable du traitement qu'il s'exécute.

Le Roi peut, après avis de la Commission, fixer les modalités relatives à la notification aux personnes concernées et à la Commission.

§ 5. Le responsable du traitement tient à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de manière à permettre à la Commission de vérifier le respect des dispositions du présent article. Cet inventaire comporte uniquement les informations nécessaires à cette fin."

HOOFDSTUK 6

Inwerkingtreding

Art. 15

De artikelen 1, 2, 12, 13 en 14 treden in werking op de eerste dag van de derde maand na die waarin ze is bekendgemaakt in het *Belgisch Staatsblad*.

De artikelen 3 tot 11 treden in werking op de eerste dag van de twaalfde maand na die waarin ze is bekendgemaakt.

30 juni 2014

Sonja BECQ (CD&V)
Nahima LANJRI (CD&V)
Roel DESEYN (CD&V)

CHAPITRE 6

Entrée en vigueur

Art. 15

Les articles 1er, 2, 12, 13 et 14 entrent en vigueur le premier jour du troisième mois qui suit celui de la publication de la présente loi au *Moniteur belge*.

Les articles 3 à 11 entrent en vigueur le premier jour du douzième mois qui suit celui de la publication de la présente loi.

30 juin 2014

Centrale drukkerij – Imprimerie centrale