INFORMATIEVEILIGHEID BEKEKEN VANUIT JURIDISCH PERSPECTIEF

Johan VANDENDRIESSCHE
Advocaat-vennoot, Crosslaw CVBA
Gastprofessor ICT-recht, Universiteit Gent (UGent)

Dit artikel werd geschreven voor het *Inforum 2014* en houdt zich aan de tekst zoals die op dat moment voorgesteld werd. De laatste evoluties voor de nieuwe Europese verordening werden dus niet opgenomen in de tekst.

- Informatieveiligheid is vanuit juridisch perspectief nog steeds niet op gecoördineerde wijze benaderd. Dit betekent echter niet dat er überhaupt geen wet- en regelgeving met betrekking tot informatieveiligheid bestaat. Naast een algemene zorgvuldigheidsnorm, die op iedereen van toepassing is, bestaan er talrijke specifieke verplichtingen met betrekking tot informatieveiligheid. De moeilijke taak van de verantwoordelijke voor informatieveiligheid bestaat erin deze regels te identificeren en correct toe te passen. De meest universeel toepasbare veiligheidsplicht kan teruggevonden worden in de Wet Verwerking Persoonsgegevens. Toch voorziet deze wet tot op heden nog niet in de aanstelling van een *"security officer"* of een meldingsplicht bij inbreuken. In het context van de herziening van het wettelijke kader met betrekking tot de verwerking van persoonsgegevens, wordt er wel druk gewerkt aan een aanzienlijke uitbreiding van de bepalingen met betrekking tot informatieveiligheid, waaronder de aanstelling van een *"data protection officer"* en een meldingsplicht bij inbreuken.

- La sécurité de l'information n'est toujours pas abordée de manière coordonnée sur le plan juridique. Cela ne signifie cependant pas qu'il n'existe pas de lois et de règlementations relatives à la sécurité de l'information. À côté d'un devoir général de diligence applicable à tous, il existe de nombreuses obligations spécifiques en lien avec la sécurité de l'information. La tâche ardue du responsable de la sécurité de l'information consiste à identifier et appliquer correctement ces règles. Le devoir de sécurité le plus largement applicable se trouve dans la loi sur le traitement des données à caractère personnel. Celle-ci ne prévoit cependant pas, pour le moment, la nomination d'un "*security officer*" ou un devoir de notification en cas de faille de sécurité. Dans le cadre de la révision du cadre juridique applicable aux traitements de données à caractère personnel, beaucoup d'attention est consacrée à un probable élargissement des dispositions relatives à la sécurité de l'information, notamment par la nomination d'un "*data protection officer*" et l'établissement d'un devoir de notification en cas de violation.

Wat is informatieveiligheid?

Informatieveiligheid is het geheel van activiteiten die worden gesteld, enerzijds met het oog op het verzekeren van de beschikbaarheid en de integriteit van informatie en informatiesystemen en, anderzijds, met het oog op het beschermen, het exclusief en het vertrouwelijk houden van informatie en informatiesystemen[1].

Informatie is immers een bijzonder waardevol gegeven in de informatiemaatschappij, niet enkel voor ondernemingen, maar ook voor publieke overheden en zelfs consumenten. Informatie wordt niet voor niets beschouwd als het nieuwe betaalmiddel van de informatiemaatschappij[2]. Het toegenomen belang en de toegenomen waarde van informatie hebben tot gevolg dat informatie veel meer dan vroeger het voorwerp uitmaakt van allerhande misdrijven, waardoor de bescherming van informatie ook steeds belangrijker wordt. Informatieveiligheid moet echter een veel ruimer doel hebben, dan enkel de zuivere bescherming ervan. Informatie maakt ook steeds meer deel uit van allerhande (bedrijfs-)activiteiten. Het doel van informatieveiligheid is dus niet enkel het beschermen van informatie tegen dreigingen van buitenaf, maar ook het verzekeren van de bruikbaarheid ervan om het volledige (economische) potentieel ervan te bereiken en te behouden.

Enkele algemene overwegingen inzake informatieveiligheid in de Belgische wetgeving

Omwille van historische redenen bevat onze wetgeving geen gecoördineerde wetgeving met betrekking tot informatieveiligheid. Heel wat wet- en regelgeving vindt immer haar oorsprong in een agrarische maatschappij, waarin informatie eerder van bijkomstig belang was. Dat weerspiegelt zich in een slechts zeer beperkte bescherming van informatie[3]. Zelfs intellectuele eigendomsrechten zijn een relatief recente ontwikkeling. Meer recente wetgeving, die voortspruit uit de informatiemaatschappij, bevat dan weer wel specifieke bepalingen met betrekking tot informatieveiligheid[4]. Deze historische ontwikkeling wordt tot op heden weerspiegeld in het beginsel dat informatie in principe vrij is en niet beschermd. De bescherming van informatie is met

andere woorden de uitzondering op de regel. Dit betekent dat het uitwerken van een juridisch beleid met betrekking tot informatieveiligheid een omvangrijke analyse vereist van diverse wet- en regelgeving.

Toch moet naast deze bijzondere wetgeving met specifieke verplichtingen inzake informatieveiligheid ook steeds teruggevallen worden op de algemene zorgvuldigheidsnorm (art. 1382-83 van het Burgerlijk Wetboek) als grondslag voor informatieveiligheid[5]. De algemene zorgvuldigheidsnorm houdt in dat elke persoon die door zijn fout of onzorgvuldigheid schade veroorzaakt aan een derde, deze schade dient te vergoeden. Er is sprake van een fout of onzorgvuldigheid, indien een normaal, voorzichtig en redelijk persoon in dezelfde feitelijke omstandigheden niet op dezelfde manier zou hebben gehandeld. In het kader van informatieveiligheid betekent dit, dat een persoon op elk ogenblik de vraag dient te stellen of een normaal, voorzichtig en redelijk persoon in dezelfde feitelijke omstandigheden al dan niet bepaalde handelingen zou stellen om de informatie die in zijn bezit is, te beveiligen en – indien dit het geval is – welke maatregelen een normaal, voorzichtig en redelijk persoon dan zou treffen. Indien het antwoord op deze vraag positief is, dan is het aangewezen de omvang van de te nemen maatregelen vast te leggen en deze maatregelen effectief te nemen teneinde aansprakelijkheid uit te sluiten of te beperken. Op die manier bewerkstelligt de algemene zorgvuldigheidsnorm een algemene, doch contextuele verplichting tot het treffen van maatregelen met het oog op informatieveiligheid. Indien een wettelijke bepaling overigens een specifieke verplichting oplegt, dan maakt de niet-naleving daarvan eveneens per definitie een tekortkoming uit van de algemene zorgvuldigheidsnorm.

De omvang van de te nemen maatregelen zal wel sterk verschillen in functie van de concrete omstandigheden. Zo zal een professionele dienstverlener met specifieke kennis inzake informatieveiligheid die gevoelige informatie verwerkt allicht een zwaardere plicht inzake informatieveiligheid hebben dan een consument die ongevoelige informatie verwerkt.

Naast de wet- en regelgeving mag echter ook de contractuele dimensie van informatieveiligheid niet uit het oog worden verloren. Zelfs in die gevallen waarin de wet- en regelgeving niet voorziet in een specifieke bescherming, kunnen personen toch via contractuele mechanismen een erg uitgebreide bescherming voorzien voor informatie. Zo kan de vertrouwelijkheid van informatie worden bewerkstelligd via zogenaamde vertrouwelijkheidsovereenkomsten, waarbij een of beide partijen zich ertoe verbinden bepaalde informatie als strikt vertrouwelijk te behandelen. Een inbreuk wordt dan gesanctioneerd via het contractueel aansprakelijkheidsrecht. Daarnaast kan ook de beschikbaarheid en de integriteit van informatie worden uitgewerkt via zogenaamde *"service level agreements"* die worden opgelegd aan dienstverleners. Zo garanderen zij bepaalde kwaliteitsvereisten met betrekking tot diensten en informatiesystemen. Ook de valorisering van informatie maakt het voorwerp uit van contractuele mechanismen. Databanken, software, boeken en andere auteursrechtelijk beschermende werken kunnen worden geëxploiteerd via licentieovereenkomsten, waarbij de ene partij aan een andere partij, al dan niet tegen betaling, bepaalde gebruiksrechten toekent.

Informatieveiligheid in de Wet Verwerking Persoonsgegevens[6]

De Wet Verwerking Persoonsgegevens mag worden beschouwd als een van de weinige wetten die een algemeen toepasbare beveiligingsplicht heeft ingevoerd. De beveiligingsplicht heeft een transversale toepassing: ze is van toepassing in alle private en publieke sectoren, ongeacht de activiteit, op voorwaarde echter dat er persoonsgegevens worden verwerkt.

De Wet Verwerking Persoonsgegevens bevat een algemene beveiligingsplicht, een aantal bijzondere beveiligingsplichten en een aantal specifieke verplichtingen bij het inschakelen van een dienstverlener (verwerker) bij het verwerken van persoonsgegevens.

De algemene beveiligingsplicht

De algemene beveiligingsplicht wordt uitgewerkt in artikel 16, §4 van de Wet Verwerking Persoonsgegevens:
"Om de veiligheid van de persoonsgegevens te waarborgen, moeten de verantwoordelijke voor de verwerking, en in voorkomend geval zijn vertegenwoordiger in België, alsmede de verwerker, de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

Op advies van de Commissie voor de bescherming van de persoonlijke levenssfeer kan de Koning voor alle of voor bepaalde categorieën van verwerkingen aangepaste normen inzake informaticaveiligheid uitvaardigen."

De Wet Verwerking Persoonsgegevens legt een verplichting op om de persoonsgegevens te beschermen tegen elke vorm van onrechtmatige verwerking, zowel toevallig als opzettelijk. De beschermingsmaatregelen moeten zowel technisch als organisatorisch zijn, maar het wordt wel aanvaard dat deze maatregelen tot op zekere hoogte onderling inwisselbaar zijn. Zo zou een relatief gebrek in organisatorische maatregelen opgevangen kunnen worden door bijkomende technische maatregelen (en omgekeerd).

De algemene beveiligingsplicht is geen absolute plicht. De verantwoordelijke voor de verwerking moet een passend beveiligingsniveau verzekeren. Om het "passend niveau" te beoordelen, wordt enerzijds gekeken naar de stand van de techniek en de kosten van de maatregelen en anderzijds naar de aard van de persoonsgegevens en de potentiële risico's.

Om de verantwoordelijke voor de verwerking te helpen, heeft de Commissie voor de bescherming van de persoonlijke levenssfeer een overzicht van referentiemaatregelen gepubliceerd. Dit document geldt als leidraad, niet als verplichting om alle erin vervatte maatregelen *de facto* te implementeren. De uit te werken veiligheidsmaatregelen hangen uitsluitend af van de bovenstaande beoordeling.

De bijzondere veiligheidsverplichtingen

Naast de algemene verplichting inzake informatieveiligheid legt de Wet Verwerking Persoonsgegevens ook vier specifieke verplichtingen inzake informatieveiligheid op.

De eerste bijzondere veiligheidsplicht heeft betrekking op de datakwaliteit. Op grond van artikel 16, §2, 1° van de Wet Verwerking Persoonsgegevens dient de verantwoordelijke voor de verwerking *"er nauwlettend over waken dat de [persoonsgegevens] worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende [persoonsgegevens], alsmede die welke zijn verkregen of verder verwerkt in strijd met de [algemene beginselen voor de rechtmatigheid van de verwerking van persoonsgegevens], worden verbeterd of verwijderd."* Deze specifieke verplichting vult het algemene beginsel inzake datakwaliteit (artikel 4, §1, 4° van de Wet Verwerking Persoonsgegevens) aan en omvat zowel een proactieve als een reactieve verplichting.

De tweede bijzondere veiligheidsplicht werkt een toegangsbeperking uit op basis van een dubbel *"need to know"*-principe (artikel 16, §2, 2° van de Wet Verwerking Persoonsgegevens). De verantwoordelijke voor de verwerking moet de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden beperken tot enkel die personen die relevant zijn en bovendien mogen de betreffende personen ook enkel toegang krijgen tot de persoonsgegevens en de verwerkingsmogelijkheden die zij nodig hebben.

De derde bijzondere veiligheidsplicht omvat een opleidingsplicht (artikel 16, §2, 3° van de Wet Verwerking Persoonsgegevens). De verantwoordelijke voor de verwerking is ertoe gehouden de personen die onder zijn gezag handelen in te lichten over de wettelijke bepalingen evenals de relevante veiligheidsvoorschriften. Deze opleidingsplicht heeft essentieel een algemeen informatief doel.

De vierde bijzondere veiligheidsplicht heeft betrekking op de doorlichting van de softwareprogramma's die worden gebruikt voor de verwerking persoonsgegevens (artikel 16, §2, 4° van de Wet Verwerking Persoonsgegevens). De verantwoordelijke voor de verwerking wordt ertoe gehouden na te gaan dat deze programma's in overeenstemming zijn met de aangegeven verwerking en dat zij niet wederrechtelijk gebruikt worden. Ook deze veiligheidsplicht dient met een zekere soepelheid te worden beoordeeld. Het zal voor de gemiddelde verantwoordelijke voor de verwerking immers juridisch, technisch of financieel niet haalbaar zijn om alle gebruikte programma's te screenen. Zo zal het b.v. bij een softwareprogramma met enkel toegang tot de objectcode moeilijk of onmogelijk zijn na te gaan wat de functionaliteiten van de software zijn. Allicht volstaat het daar om een contractuele garantie te bedingen met betrekking tot de functionaliteiten van de software en de afwezigheid van eventuele ongedocumenteerde functionaliteiten.

De maatregelen die moeten worden genomen bij het inschakelen van een verwerker

Indien de verantwoordelijke voor de verwerking bij de verwerking van persoonsgegevens gebruik maakt van een dienstverlener (de verwerker), dan dient de verantwoordelijke voor de verwerking bijkomende maatregelen te nemen (artikel 16, §1 van de Wet Verwerking Persoonsgegevens).

In eerste instantie moet de verantwoordelijke voor de verwerking een betrouwbare verwerker kiezen. Dit veronderstelt dat de verantwoordelijke

voor de verwerking een minimale achtergrondcontrole van de verwerker doorvoert in het kader van het selectieproces.

De verantwoordelijke voor de verwerking moet, in tweede instantie, een geschreven overeenkomst (papier of elektronisch) aangaan met de verwerker, die bovendien de te nemen veiligheidsmaatregelen en de aansprakelijkheid van de verwerker moet vastleggen.

De verantwoordelijke voor de verwerking moet ten slotte ook bedingen dat de verwerker enkel mag handelen in opdracht van de verantwoordelijke voor de verwerking, overeenkomstig diens instructies. De overeenkomst moet dus in het bijzonder elk gebruik van de persoonsgegevens voor eigen doeleinden van de verwerker uitsluiten.

De aanstelling van een aangestelde voor de gegevensbescherming (*"data protection officer"*)

Hoewel de Wet Verwerking Persoonsgegevens de mogelijkheid laat om, bij koninklijk besluit uitgevaardigd na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, een verplichting op te leggen tot aanstelling van een zgn. *"data protection officer"*, moet worden vastgesteld dat het Belgische wettelijke kader hieraan geen uitwerking heeft gegeven[7].

In tegenstelling tot sommige andere EU-lidstaten werd geen specifiek wettelijk of regelgevend kader uitgewerkt met betrekking tot de aanstelling, de taak, het statuut en de gevolgen van de aanstelling van een *"data protection officer"*. Dit betekent dat de aanstelling van een *"data protection officer"* geen enkele impact heeft op de rechten en plichten van de verantwoordelijke voor de verwerking, uitgezonderd eventueel de evaluatie van het passend beveiligingsniveau dat de verantwoordelijke voor de verwerking moet garanderen op grond van artikel 16, §4 van de Wet Verwerking Persoonsgegevens.

De nauwst aansluitende verplichting die in het Belgische recht kan worden gevonden, is de verplichting tot aanstelling van een veiligheidsconsulent. Deze verplichting kan worden teruggevonden in diverse wetgeving o.a. met betrekking tot de werking van de sociale zekerheid en ziekenhuizen. Toch kan de rol van deze veiligheidsconsulent niet volledig gelijkgeschakeld worden met de rol van een *"data protection officer"*.

In het Voorstel voor een verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), dat thans het voorwerp uitmaakt van wetgevend debat, is er wel uitdrukkelijk een verplichting voorzien tot aanstelling van een *"data protection officer"*. In die tekst is er sprake van een *"functionaris voor gegevensbescherming"*, die o.a. moet instaan voor advies, toezicht, bewaring van documenten en het optreden als contactpunt met de toezichthoudende overheden. De aanstelling van een *"data protection officer"* zou verplicht worden voor overheden, grote ondernemingen en verantwoordelijken voor de verwerking of verwerkers met verwerkingen die regelmatige en stelselmatige observatie van betrokkenen vereisen.

Meldingsplicht bij veiligheidsincidenten

Tot op heden voorziet de Wet Verwerking Persoonsgegevens niet in een verplichte melding van veiligheidsincidenten bij de Commissie voor de bescherming van de persoonlijke levenssfeer. Een dergelijke meldingsplicht staat nochtans hoog op de verlanglijst van de Commissie voor de bescherming van de persoonlijke levenssfeer[8].

De Wet Verwerking Persoonsgegevens als rem voor informatieveiligheid

Het feit dat de Wet Verwerking Persoonsgegevens als een van de weinige Belgische wetten een uitgewerkte regeling inzake informatieveiligheid bevat, verhindert nochtans niet dat de Wet Verwerking Persoonsgegevens ook als rem op informatieveiligheid inwerkt.

Bij de implementatie van technische veiligheidsmaatregelen zal immers ook zelf met de beperkingen van de Wet Verwerking Persoonsgegevens rekening moeten worden gehouden, indien de technische veiligheidsmaatregelen zelf een verwerking van persoonsgegevens omvatten.

Er zijn talrijke maatregelen die het voorwerp hebben uitgemaakt van een advies van de Commissie voor de bescherming van de persoonlijke levenssfeer of de Europese Werkgroep Artikel 29. Daarbij kan o.a. worden gedacht aan werknemerscontrole via cameratoezicht of toezicht op de elektronische communicatie, (bewakings-)camera's, klokkenluidersregelingen, zwarte lijsten, toegangs- en identiteitscontrole (al dan niet via biometrische toepassingen), achtergrondcontrole en archivering van persoonsgegevens[9].
De niet-naleving van deze wettelijke beperkingen kan een impact hebben op de mogelijkheid om het aldus (onwettig) verkregen bewijs te gebruiken in het kader van een rechtszaak.

Toekomst

Het wettelijke kader met betrekking tot de verwerking van persoonsgegevens wordt momenteel herzien. De Europese Commissie heeft de intentie om de bestaande Europese Richtlijn 1995/46/EG[10] te vervangen door een verordening, die rechtstreeks inwerkt in de rechtsorde van de EU-lidstaten[11]. De verordening doorloopt op dit ogenblik het Europees wetgevend proces.
De huidige ontwerptekst van de verordening voorziet een hele reeks vernieuwingen met betrekking tot informatieveiligheid. Naast een reeks bijkomende verplichtingen, waaronder de aanstelling van een *"data protection officer"*, een meldingsplicht bij veiligheidsincidenten en de noodzaak van een impactanalyse inzake privacy met betrekking tot de verwerking van persoonsgegevens, worden een aantal bijkomende principes nu fundamenteel ingebed in de tekst van de verordening.

De voornaamste nieuwe principes zijn *"privacy by design"* en *"privacy by default"*. Deze beginselen omvatten de verplichting voor de verantwoordelijke voor de verwerking om maatregelen te treffen om ervoor te zorgen dat alle verwerking in lijn zijn en blijven met de regelgeving en de rechten van de betrokkenen, evenals dat persoonsgegevens niet standaard ter beschikking worden gesteld aan een onbeperkt aantal personen.
Toch is het op dit ogenblik nog te vroeg om een definitief beeld te krijgen op de finale tekst van de verordening. Het wetgevend proces is immers nog niet voltooid.

Conclusie

Het Belgisch wetgevend kader weerspiegelt duidelijk de evolutie die de maatschappij heeft gekend: van agrarische maatschappij naar industriele maatschappij tot informatiemaatschappij. De wetgever heeft gaandeweg het belang van informatie onderkend en de toepasselijke wetgeving aangepast of ingevoerd. Dit is echter niet op gecoördineerde wijze gebeurd, zodat het moeilijk blijft alle wet- en regelgeving met betrekking tot informatieveiligheid in kaart te brengen. De nieuwe stappen van de Belgische en de Europese wetgever tonen echter duidelijk aan dat informatieveiligheid steeds hoger in de prioriteitenlijst komt te staan[12]. Ondernemingen en overheden houden er dus best rekening mee dat zij bijkomende inspanningen in het kader van informatieveiligheid zullen moeten leveren.

Johan Vandendriessche
Crosslaw CVBA
Marsveldplein 2
1050 Brussel
j.vandendriessche@crosslaw.be
http://www.crosslaw.be

November 2014

Noten

1 Zie b.v. Bowen, Pauline; Hash, Joan; Wilson, Mark. *Information Security Handbook: A Guide for Managers* [online]. NIST, 2006 (geraadpleegd op 22 mei 2015). <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.

2 World Economic Forum. *Personal Data: The Emergence of a New Asset Class* [online]. World Economic Forum, 2011 (geraadpleegd op 22 mei 2015).
<http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>.

3 Zie b.v. artikel 458 van het Strafwetboek (beroepsgeheim) en artikel 309 van het Strafwetboek (fabrieksgeheim).

4 Zie b.v. Wet van 28 november 2000 inzake informaticacriminaliteit.

5 Voor meer informatie met betrekking tot de algemene zorgvuldigheidsnorm: De Tavernier, Pieter, *Buitencontractuele aansprakelijkheid voor schade veroorzaakt door minderjarigen*. 1ste uitgave. Intersentia, 2006. ISBN 978-90-5095-516-4.

6 Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Wet Verwerking Persoonsgegevens).
Voor uitgebreide informatie inzake de Wet Verwerking Persoonsgegevens: De Bot, Dirk, *Verwerking van persoonsgegevens*, 1ste uitgave. Kluwer, 2001. ISBN 90-5583-773-3; Van Gossum, Kirsten; Vandendriessche, Johan, De bescherming van de persoonlijke levenssfeer bij internetgerelateerde verwerkingen: algemeen overzicht en praktische toepassingen. In Decorte, Rogier (ed.) *Praktijkboek Recht en Internet.* Uitgeverij Vanden Broele, 2014. ISBN 978-90-496-1072-2.

7 Artikel 17*bis*, tweede alinea van de Wet Verwerking Persoonsgegevens voorziet de mogelijk om de aanstelling van een "*aangestelde voor de gegevensbescherming*" verplichtend op te leggen, bij koninklijk besluit uitgevaardigd na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, doch deze uitvoeringsmaatregel is tot op heden niet genomen.

8 Commissie voor de bescherming van de persoonlijke levenssfeer. *Aanbeveling nr. 01/2013 van 21 januari 2013 betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken* [online]. Commissie voor de bescherming van de persoonlijke levenssfeer, 2013 (geraadpleegd op 22 mei 2015). <http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_01_2013.pdf>.

9 Deze adviezen en aanbevelingen zijn raadpleegbaar op de websites van deze entiteiten: Commissie voor de bescherming van de persoonlijke levenssfeer, *Privacycommission.be* [online] <http://www.privacycommission.be/nl> en Artikel 29 Werkgroep, *Article 29 Working Party* [online] <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> (beiden geraadpleegd op 22 mei 2015).

10 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Europese Unie. *Toegang tot het recht van de Europese Unie* [online] <http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:31995L0046&from=NL>) (geraadpleegd op 22 mei 2015).

11 Zie voor meer informatie inzake de modernisering van het regelgevend kader inzake de verwerking van persoonsgegevens: Europese Commissie. *Bescherming van persoonlijke gegevens* [online] <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> (geraadpleegd op 22 mei 2015).

12 Zo diende de Europese Commissie op 7 februari 2013 een voorstel voor richtlijn in, houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Europese Unie te waarborgen (COM (2013) 48 final): Europese Unie. *Toegang tot het recht van de Europese Unie* [online] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:NL:PDF> (geraadpleegd op 22 mei 2015).