

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### Bescherming van Persoonsgegevens

de Villenfagne, Florence

*Published in:*

Elektronische Handel : juridische en praktische aspecten

*Publication date:*

2004

*Document Version*

le PDF de l'éditeur

[Link to publication](#)

*Citation for pulished version (HARVARD):*

de Villenfagne, F 2004, Bescherming van Persoonsgegevens. in *Elektronische Handel : juridische en praktische aspecten*. UGA, Heule, pp. 167-182.

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

## HOOFDSTUK 7: BESCHERMING VAN PERSOONS- GEGEVENS

Florence de Villenfagne

*Juriste gespecialiseerd in informaticarecht en communicatietechnologie*

### I. INLEIDING

Het gebruik van informatie- en communicatietechnologie (ICT) en meer bepaald van het Internet heeft de toegang tot het privé-leven en tot persoonsgegevens compleet veranderd. Met amper enkele «klikken» op een scherm vertelt de Internetter aan een onbekende zijn hobby's, interesses en politieke gezindheid, en zijn godsdienstige of levensbeschouwelijke overtuiging. Dankzij bepaalde technieken zoals het gebruik van cookies wordt het voor ondernemingen kinderspel om de profielen van Internetters te achterhalen en hen daarna passende – of minder passende – producten aan te bieden.

Maar het verzamelen, ordenen, gebruiken of anders bewerken van persoonsgegevens is sinds 1992<sup>1</sup> in België onderworpen aan een specifieke wetgeving. De regels die destijds in de context van mainframes werden opgesteld hebben transparantie, rechtmatig beheer en controle over bewerkingen van persoonsgegevens als doel. Ze werden in 1998 nog aangepast naar aanleiding van de Europese Richtlijn van 24 oktober 1995<sup>2</sup> die de materie van de bescherming van persoonsgegevens in de Europese Unie min of meer harmoniseert<sup>3</sup> en die in alle nationale wetgevingen van de Lidstaten<sup>4</sup> omgezet zou moeten zijn.

Deze regels moeten het vandaag opnemen tegen Big Brother en wilde marketing in een Internet context.

<sup>1</sup> Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (gewijzigd door de wet van 11 december 1998), *B.S.*, 18 maart 1993; gecoördineerde versie is beschikbaar op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer, [www.privacy.fgov.be](http://www.privacy.fgov.be).

<sup>2</sup> Richtlijn 95/46/CE 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, *PB*, L 281, 23 november 1995, p. 31.

<sup>3</sup> Doordat de Lidstaten een bepaalde vrijheid hebben bij het omzetten van de Richtlijn, zijn de nationale teksten niet hetzelfde.

<sup>4</sup> Dit is jammer genoeg lang niet het geval. Raadpleeg de samenvattende tabel over de toestand ter zake in de verschillende landen van de Unie op het volgende adres: [http://europa.eu.int/comm/internal\\_market/privacy/law/implementation\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm)

In België werd dus op 8 december 1992 een wettelijk kader gegeven aan de verwerking van persoonsgegevens. Dit kader wordt hierna besproken zonder evenwel de wet volledig te analyseren.

De bedoeling van dit hoofdstuk is immers enkel een praktische uitleg te geven aan ondernemingen, die via hun website persoonsgegevens verzamelen en daarna verwerken, over de wijze waarop deze verwerking moet gebeuren. Het is niet de bedoeling om elke uitzondering uiteen te zetten. De hierna komende «high level guidelines» staan dus niet in de weg dat de ondernemingen bijkomend juridisch advies dienen in te winnen.

## II. WANNEER DIENT EEN ONDERNEMING DE BELGISCHE WET VAN 1992 TOE TE PASSEN?

Eén van de meest complexe punten die in de materie van bescherming van persoonsgegevens onderzocht moet worden betreft de omstandigheden waarin een onderneming een wetgeving tot bescherming van persoonsgegevens moet naleven en het bepalen van de nationale wet die van toepassing is.

### A. De toepassing van de wetgeving tot bescherming van persoonsgegevens<sup>5 6</sup>

Algemeen gesproken mag men stellen dat een onderneming een wetgeving tot bescherming van persoonsgegevens moet naleven, als ze persoonsgegevens verwerkt op een geheel of gedeeltelijk geautomatiseerde manier, evenals op een niet geautomatiseerde manier als de gegevens in een «bestand»<sup>7</sup> worden verzameld.

De betreffende wetgeving is dus enkel van toepassing als er sprake kan zijn van persoonsgegevens, met andere woorden van «iedere informatie betreffende een geïdentificeerde of identificeerbaar<sup>8</sup> natuurlijke persoon»<sup>9</sup>.

<sup>5</sup> Artikel 3, Richtlijn 95/46/EG, a.c.

<sup>6</sup> In deze sectie gebruiken we de definities zoals ze in de tekst van de Richtlijn 95/46/EG voorkomen. Deze verschillen weinig van de definities die voorkomen in de Belgische wet, die in de overige secties zullen worden gebruikt.

<sup>7</sup> «Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn». Artikel 2, Richtlijn 95/46/EG, a.c.

<sup>8</sup> als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

<sup>9</sup> Artikel 2, Richtlijn 95/46/EG, a.c.

### Voorbeelden van persoonsgegevens:

- naam, e-mail adres en andere gegevens die per formulier via een website worden opgevraagd;
- cookies<sup>10</sup>: deze worden in principe<sup>11</sup> op de harde schijf van de Internetter opgeslagen, en telkens als de Internetter de site van de onderneming opnieuw bezoekt worden ze teruggestuurd naar de server die ze daar plaatste. Dankzij deze computeridentificatietechniek is het mogelijk een profiel op te stellen van de Internetter, dat bij ieder nieuw bezoek aangevuld wordt<sup>12</sup>;
- genummerde gegevens die een identificeerbare persoon betreffen<sup>13</sup>.

### Worden uitgesloten uit het toepassingsgebied van de wet:

- anonieme gegevens.

Vervolgens moeten die gegevens een verwerking ondergaan, m.a.w. een «bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, 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»<sup>14</sup>.

<sup>10</sup> Een *cookie* is een klein tekstbestand of een lijst met lettertekens die overeenstemmen met een code bepaald door de uitzender (de «server»).

<sup>11</sup> Een *cookie* kan tijdelijk zijn (bezoek-cookie) of blijvend. In het eerste geval wordt de cookie slechts tijdelijk opgeslagen in de computer van de Internetter. Hij verdwijnt zodra de Internetter zijn bezoek beëindigt. In het tweede geval wordt hij opgeslagen op de harde schijf van de computer van de Internetter, en bij ieder nieuw bezoek teruggestuurd naar de server van oorsprong die bijgevolg geleidelijk steeds meer informatie verzamelt over de Internetter.

<sup>12</sup> Sinds kort bestaat er op Europees niveau een specifieke bepaling over het gebruik van cookies. Het gebruik van cookies wordt slechts toegestaan op voorwaarde dat ze voor een legitiem doel bestemd zijn, dat de betrokken gebruiker duidelijke en volledige informatie krijgt en op voorwaarde dat de betrokken gebruiker de mogelijkheid heeft om de cookie te weigeren. Zulks vormt echter geen beletsel voor het gebruiken van cookies met als uitsluitend doel de uitvoering of vergemakkelijking van de verzending van gegevens over een elektronische-communicatienetwerk, of, indien strikt noodzakelijk, voor de levering van een uitdrukkelijk door de abonneegebruiker gevraagde dienst van de informatiemaatschappij. Aan toegang tot specifieke inhoud van een website kan de voorwaarde worden verbonden dat een cookie bewust aanvaard wordt indien het voor een legitiem doel gebruikt wordt. Het betreffende artikel 5.3 van de Richtlijn 2002/58/EG van 12 juli 2002 betreffende privacy en elektronische communicatie dient echter nog in de verschillende nationale wetgevingen omgezet te worden.

<sup>13</sup> «Anonieme» genummerde gegevens waarvan de eigenaar teruggevonden kan worden aan de hand van een ander bestand dat de namen bevat van de eigenaars van de gegevens en de overeenstemmende nummers, zijn geen anonieme gegevens, maar gecodeerde gegevens. Het zijn dus persoonsgegevens.

<sup>14</sup> Artikel 2, Richtlijn 95/46/EG, a.c.

*Voorbeelden van verwerkingen:*

- verzamelen van persoonsgegevens via een formulier op een website;
- gebruiken van persoonsgegevens om een boodschap te sturen aan de betrokken persoon;
- opnemen en ordenen van persoonsgegevens in een databank;
- bijwerken, wissen, overbrengen van persoonsgegevens naar een andere onderneming, een dochteronderneming, enz.

*Worden uitgesloten uit het toepassingsgebied van de wet:*

- persoonsgegevens die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verwerkt.

**B. Toepassing van de Belgische wet van 1992**

Indien een onderneming effectief persoonsgegevens verwerkt, moet zij nog enerzijds bepalen of zij de verantwoordelijke voor de verwerking is, en anderzijds welke (nationale) wet zij moet naleven. Deze sectie is aan dit laatste punt gewijd. De hoedanigheid van de verantwoordelijke voor de verwerking wordt besproken in de volgende sectie.

Zoals we eerder<sup>15</sup> al hebben onderstreept, is door de goedkeuring van Richtlijn 95/46 ter zake een zekere harmonisatie in de verschillende Lidstaten mogelijk geworden. Binnen de Europese Unie zou de kwestie van de toepasselijke nationale wet dus van weinig belang moeten zijn. Nochtans is het noodzakelijk – gelet op de verschillen die tussen de nationale wetgevingen bestaan – de juiste toepasselijke wet te bepalen. We onderzoeken hierna in welke omstandigheden de Belgische Wet van toepassing is<sup>16</sup>.

Het bepalen van de toepassing van de Belgische Wet op een verwerking van persoonsgegevens is gevestigd op artikel 3bis van de Wet van 8 december 1992<sup>17</sup>. De toepassing van deze regel is in de praktijk uiterst ingewikkeld. Omdat het niet onze bedoeling is deze uitvoerig regel te bespreken, zullen we

<sup>15</sup> Zie noot nr. 3.

<sup>16</sup> Let wel dat het mogelijk kan zijn dat verschillende nationale wetgevingen van toepassing zijn op een zelfde verwerking.

<sup>17</sup> «Deze wet is van toepassing:

1° op de verwerking van persoonsgegevens die wordt verricht in het kader van de effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking op het Belgisch grondgebied of op een plaats waar de Belgische wet uit hoofde van het internationaal publiekrecht van toepassing is;

2° op de verwerking van persoonsgegevens door een verantwoordelijke die geen vaste vestiging op het grondgebied van de Europese Gemeenschap heeft, indien voor de verwerking van persoonsgegevens gebruik gemaakt wordt van al dan niet geautomatiseerde middelen die zich op het Belgisch grondgebied bevinden, andere dan degene die uitsluitend aangewend worden voor de doorvoer van de persoonsgegevens over het Belgisch grondgebied. [...]».

ons beperken tot het uitleggen van de basisregel door het geven van voorbeelden van wat volgens ons de meest voorkomende gevallen zijn<sup>18</sup>.

Beknopt kan de regel van toepassing van de Belgische Wet als volgt verwoord worden:

Indien de verantwoordelijke voor de verwerking gevestigd is in één van de lidstaten van de Europese Unie, volstaat het uit te maken of de verwerking van de persoonsgegevens plaatsheeft in het kader van effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking in België.

Om deze regel toe te passen dient er dus uitgemaakt te worden:

- wie de verantwoordelijke voor de verwerking is (we zullen dit punt bespreken in de volgende sectie);
- of de verantwoordelijke een vaste vestiging heeft in België; ongeacht met welke rechtsvorm (gewoon bijkantoor of dochteronderneming)<sup>19</sup>;
- of de verwerking binnen het kader valt van de effectieve en daadwerkelijke activiteiten van die vaste vestiging in België.

De Belgische Wet zal dus van toepassing zijn op de verwerking van persoonsgegevens door een dochteronderneming in België van een Nederlandse moedermaatschappij indien de Belgische entiteit persoonsgegevens verzamelt via haar eigen («Belgische») website ([www.maatschappij.be](http://www.maatschappij.be)) en ze daarna beheert.

Dat de moederonderneming een Nederlandse maatschappij is en dat de dochteronderneming via haar site gegevens kan verzamelen over Nederlandse, Zweedse of Zambiaanse Internetters is dus van weinig belang.

Daarentegen zal de Belgische Wet niet van toepassing zijn indien een Duitse onderneming, die ook een dochteronderneming in België zou hebben, rechtstreeks persoonsgegevens verzamelt via een website [www.unternehmung.de](http://www.unternehmung.de) die geheel door de Duitse moedermaatschappij beheerd wordt (de server ligt in Duitsland, enz.). Al heeft de moedermaatschappij een vaste vestiging in België en kunnen gegevens over Belgische Internetters verzameld worden, valt het verzamelen van gegevens niet binnen het kader van de effectieve en daadwerkelijke activiteiten van de Belgische entiteit en is de Belgische Wet bijgevolg niet van toepassing.

Ingewikkelder is het een antwoord te vinden op de vraag of de Belgische Wet van toepassing is, als de Nederlandse moedermaatschappij beslist een algemene databank te maken van alle klanten en Internetbezoekers van de groep.

<sup>18</sup> In dit hoofdstuk bespreken we hoofdzakelijk gevallen met betrekking tot de eerste alinea an artikel 3bis.

<sup>19</sup> Zie overweging 19 van de Europese Richtlijn 95/46/EG, a.c.

Dan is het waarschijnlijk dat zij elk van haar dochterondernemingen ermee belast de gegevens over hun plaatselijke klanten en bezoekers te verzamelen om ze vervolgens naar Nederland door te sturen voor verdere verwerking door de moedermaatschappij. O.i. is de Belgische Wet van toepassing wat de gegevens betreft over de klanten/Internetbezoekers die door de Belgische dochteronderneming worden verzameld, voor zover die verwerking gebeurt in het kader van de effectieve en daadwerkelijke activiteiten van de vaste vestiging van de moedermaatschappij in België. Toch ontslaat dit o.i. de moedermaatschappij niet van de verplichting de Nederlandse Wet toe te passen op het globale bestand met de gegevens van alle dochterondernemingen (in ieder geval wat de aangifte betreft die moet gedaan worden aan het Nederlandse College Bescherming Persoonsgegevens). Wat de andere door de wet bepaalde verplichtingen (inlichting van de betrokkene, enz.) betreft, zullen deze merendeel reeds vervuld zijn door elk van de dochterondernemingen (wetten van andere Lidstaten wijken immers niet zoveel van elkaar af).

Tot slot wordt artikel 3bis aangevuld met een regel bestemd voor ondernemingen die gelegen zijn buiten de Europese Unie. Als een Australische onderneming persoonsgegevens verzamelt in België (zij doet bijvoorbeeld een beroep op een Belgisch callcenter dat de gegevens verzamelt en naar Australië verstuurt), dan zal de Belgische Wet eveneens van toepassing zijn.<sup>20</sup>

Deze voorbeelden tonen de complexiteit aan van situaties waarin sommige multinationals zich kunnen bevinden wanneer ze persoonsgegevens verwerken.

### III. WAT ZIJN DE VERPLICHTINGEN VAN DE VERANTWOORDELIJKE VOOR DE VERWERKING?

#### A. De verantwoordelijke en de verwerker

##### 1. De verantwoordelijke voor de verwerking

De verantwoordelijke voor de verwerking is «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»<sup>21</sup>.

Met andere woorden is de verantwoordelijke de onderneming/persoon die de beslissingsbevoegdheid over de verrichte verwerking heeft (diegene die de categorieën van gegevens bepaalt, het gebruik ervan bepaalt, enz.). Hij staat in voor het naleven van de wettelijke verplichtingen inzake de persoonsgegevens die hij verwerkt of die hij door een derde laat verwerken.

<sup>20</sup> Zie alinea 2 van artikel 3bis van de Wet, *ac.*, noot 17.

<sup>21</sup> Artikel 1, Wet van 1992.

## 2. De verwerker

Van de zijde van de verantwoordelijke kunnen andere personen of ondernemingen betrokken zijn bij de verwerking van gegevens. Een callcenter bijvoorbeeld dat alle personen van een bestand opbelt voor rekening van een andere onderneming, of een onafhankelijk informaticabedrijf dat gespecialiseerd is in de aanpassing van adressenbestanden (wijziging van de postnummers, herschikking van de bestanden, collationering, bijwerking, organisatie van mailings, enz.). Deze entiteiten zijn niet de verantwoordelijken voor de verwerking, het zijn toeleveranciers of verwerkers<sup>22</sup> die slechts mogen handelen in opdracht van de verantwoordelijke.

### B. De verplichtingen van de verantwoordelijke voor de verwerking: algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens

#### 1. Wanneer mogen persoonsgegevens verwerkt worden<sup>23</sup>?

De wet van 1992 voorziet zes omstandigheden waarin persoonsgegevens verwerkt mogen worden<sup>24</sup>. Gegevens die via het Internet worden verzameld, vallen meestal onder de twee eerste of de laatste hiervan<sup>25</sup>, d.z.:

- (i) ofwel heeft de betrokkene «zijn ondubbelzinnige toestemming» gegeven voor de verwerking;
- (ii) ofwel is de verwerking «noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen»;

<sup>22</sup> «De natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt, met uitsluiting van de personen die onder rechtstreeks gezag van de verantwoordelijke voor de verwerking gemachtigd zijn om de gegevens te verwerken.»

<sup>23</sup> Artikel 5, Wet van 1992.

<sup>24</sup> Let wel dat de verwerking van gevoelige gegevens («waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen), gezondheidsgegevens en gegevens «inzake geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten» verboden zijn, behalve onder de omstandigheden bepaald onder artikelen 6 tot 8 van de Wet van 1992.

<sup>25</sup> De andere omstandigheden waarin persoonsgegevens verwerkt mogen worden zijn (zie artikel 5 van de Belgische Wet):

- «wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verantwoordelijke voor de verwerking is onderworpen door of krachtens een wet, een decreet of een ordonnantie;
- wanneer de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verantwoordelijke voor de verwerking of aan de derde aan wie de gegevens worden verstrekt.»

(iii) ofwel is de verwerking «noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor de verwerking of van de derde aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van de wet, niet zwaarder doorwegen».

Met andere woorden, indien een verantwoordelijke persoonsgegevens uitsluitend gebruikt in het kader van de uitvoering van een bestelling van producten (de gegevens zijn noodzakelijk om het product te kunnen sturen, om een factuur te kunnen opstellen, om after sales diensten te verlenen, enz.) dient hij geen toestemming aan de Internetter te vragen om diens gegevens te verwerken. Verder hoeft de verantwoordelijke ook geen toestemming te vragen wanneer de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigde belang die hij heeft op voorwaarde dat het belang of de fundamentele rechten en vrijheden van de betrokkene niet zwaarder doorwegen. Elke verantwoordelijke zal geneigd zijn deze laatste bepaling (de belangenafweging) in te roepen om persoonsgegevens te verwerken zonder de toestemming van de betrokkene. Er dient echter opgemerkt te worden dat de bepaling strikt geïnterpreteerd moet worden en niet mag worden gebruikt om de verplichting om de toestemming van de betrokkene te bekomen te omzeilen.

## 2. Hoe dienen persoonsgegevens verwerkt te worden<sup>26</sup>?

Persoonsgegevens dienen ten eerste eerlijk en rechtmatig verwerkt te worden. Dit houdt o.a. in dat persoonsgegevens nooit in strijd met een wet verwerkt mogen worden. Dit betreft echter niet alleen de bepalingen van de wet van 1992 zelf. Ook andere wetgeving, zoals de «Convention for the Protection of Human Rights and Fundamental Freedoms», de Grondwet, Strafwetbepalingen (artikel 314bis die betrekking heeft op het beschermen van privé-communicatie) of de Wet van 21 maart 1991 (Hoofdstuk X: «geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer») zijn hier terzake.

Ten tweede dienen persoonsgegevens «voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden.» Voor een verantwoordelijke is het dus van belang dat, op het moment van het verstrekken van informatie aan de betrokkene, de doeleinden zo wijd mogelijk worden omschreven, zonder echter te algemeen te zijn (ze moeten «welbepaald» zijn). De verantwoordelijke dient hiervoor op voorhand de verschillende doeleinden in te beelden waarvoor hij de gegevens zal

gebruiken: klantenbeheer, marketingdoeleinden (informatie over producten, diensten, evenementen, enquêtes, ...), statistieken, zijn hier enkele voorbeelden<sup>27</sup> van.

De gegevens die verzameld worden moeten «toereikend, terzake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt». Ze mogen «in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer worden bewaard dan (...) noodzakelijk is». Cookies met vervaldatum in 2043 voldoen zeker niet aan deze criteria.

*In fine* rust ook op de verantwoordelijke voor de verwerking de plicht om te zorgen dat de gegevens «nauwkeurig zijn en, zo nodig, worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren». Om aan deze verplichting te voldoen dient de verantwoordelijke technische en organisatorische maatregelen te nemen. Hij kan b.v. ieder jaar contact nemen met de betrokkenen om na te gaan of zijn/haar gegevens nog geldig zijn, een «zwarte lijst» met de namen van de mensen die zich tegen het gebruik van hun gegevens voor marketingdoeleinden hebben verzet kan opgesteld worden, enz.

## 3. Gegevens gebruiken voor direct marketing

Ondernemingen die persoonsgegevens via hun web site verzamelen teneinde deze te gebruiken voor het versturen van elektronische reclame dienen de nieuwe wetgeving inzake spamming na te leven. Op basis van artikel 14 van de Belgische Wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij<sup>28</sup> en van het Koninklijk Besluit van 4 april 2003 tot reglementering van het verzenden van reclame per elektronische post<sup>29</sup> dienen de ondernemingen als volgt te handelen:

- elektronische post<sup>30</sup> voor reclame enkel gebruiken indien ze een voorafgaande, vrije, specifieke en geïnformeerde toestemming hebben gekregen van de betrokken persoon (opt-in oplossing). Deze toestemming mag

<sup>27</sup> Andere voorbeelden van doeleinden zijn te vinden in de aangifte die aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer gedaan moet worden, zie [www.privacy.fgov.be](http://www.privacy.fgov.be).

<sup>28</sup> Gebaseerd op Artikel 7 van de Richtlijn 2000/31/EG van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt.

<sup>29</sup> Gebaseerd op Artikel 13 van de Richtlijn 2002/58/EG van 12 juli 2002 betreffende privacy en elektronische communicatie.

<sup>30</sup> Het sturen van reclame via SMS (Short Message System) wordt hier ook mee bedoeld.

<sup>26</sup> Artikel 4, Wet van 1992.

natuurlijk niet per ongevraagde elektronische post gevraagd worden, dit zou ook als spamming beschouwd worden;

*uitzondering (opt-out oplossing): men is vrijgesteld de voorafgaande toestemming te vragen bij zijn klanten, indien (i) hun elektronische contactgegevens op wettelijke wijze verkregen werden in het kader van de verkoop van een product of een dienst; (ii) enkel reclame wordt gestuurd voor gelijkaardige producten of diensten die men zelf levert; en (iii) op het ogenblik waarop hun elektronische contactgegevens worden verzameld, men steeds de mogelijkheid geeft aan zijn klanten om zich kosteloos en op gemakkelijke wijze tegen de uitbating te verzetten*

- ervoor zorgen dat ze het bewijs kunnen leveren dat de reclame via elektronische post werd gevraagd. Het is dus aangewezen een schriftelijk of elektronisch bewijs bij te houden;
- steeds een duidelijke en begrijpelijke informatie verschaffen over het recht zich te verzetten tegen het ontvangen, in de toekomst, van reclame, en een geschikt middel ter beschikking stellen om dit recht langs elektronische weg uit te oefenen;
- binnen een redelijk termijn een ontvangstbewijs elektronisch sturen aan de betrokken persoon dat de registratie van zijn aanvraag tot verzetting tegen het ontvangen van reclame geregistreerd werd; binnen een redelijk termijn de nodige maatregelen nemen om deze wil na te leven; en een lijst bijwerken met personen die gevraagd hebben geen elektronisch post te ontvangen.

### C. De verplichtingen van de verantwoordelijke voor de verwerking: Front Office en Back Office verplichtingen

Krachtens de Belgische Wet vallen twee soorten van verplichtingen toe aan de verantwoordelijke voor de verwerking. We zullen deze de verplichtingen van het Front Office en van het Back Office noemen, respectievelijk de zichtbare verplichtingen die de persoon betrokken bij de persoonsgegevens ondervindt en de verplichtingen waarvan hij geen directe kennis heeft.

#### 1. Front Office verplichtingen

##### 1.1. Wettelijke informatie

Een onderneming die persoonsgegevens verzamelt (ongeacht of dat via haar website, door een enquête, wedstrijd of met andere middelen gebeurt), heeft de verplichting ten minste de volgende informatie te verstrekken aan de betrokken persoon, en dit uiterlijk op het ogenblik dat de gegevens worden

verkregen (behalve als de persoon er reeds van in kennis is gesteld via andere kanalen):

- de naam en het adres van de verantwoordelijke voor de verwerking;
- de doeleinden van de verwerking;
- het bestaan van een recht om zich op verzoek en kosteloos te verzetten tegen de voorgenomen verwerking van hem betreffende persoonsgegevens indien de verwerking verricht wordt met het oog op direct marketing;
- bijkomende informatie (behalve als dit niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen):
  - de ontvangers of categorieën van ontvangers van de gegevens;
  - het al dan niet verplichte karakter van het antwoord en de eventuele gevolgen van niet-beantwoording;
  - het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem betrekking hebben<sup>31</sup>.

Deze informatie komt doorgaans voor in een clause die vermeld wordt op de inzamelingsformulieren of Internetpagina's waarop persoonsgegevens worden verzameld. Ook kan dit vermeld staan in een «privacybeleid» dat bovendien duidelijk de rechten van de betrokken personen en de manier waarop ze kunnen worden uitgeoefend uitlegt (on line, met de gewone post, per fax enz.), alsook informatie verschaft over het desgevallend gebruik van cookies<sup>32</sup>.

Tot slot is het verkieslijk die informatie te herhalen op de mailings, elektronische post en andere brieven die aan de betrokken personen gericht worden.

#### 1.2. De rechten van de betrokkene

Zoals vermeld in de clause waarover we hierboven (III.C.1.1., al. 2) spraken, heeft de betrokken persoon drie bijzondere rechten, die gerespecteerd moeten worden: het recht om **toegang** te krijgen tot zijn gegevens, het recht om de gegevens over hem kosteloos te **verbeteren**, en het recht om zich tegen sommige verwerkingen te **verzetten**. Het is aangewezen binnen de onderneming doeltreffende procedures in te stellen om deze rechten te respecteren. De aanwijzing van een verantwoordelijke persoon, een contactpersoon, van een te volgen procedure bij verzet, de aanmaak van een databank met personen die hun recht op verzet hebben uitgeoefend (om zeker te zijn dat hun gegevens niet meer voor de bepaalde doeleinden waartegen zij zich

<sup>31</sup> Zie ook de informatie omtrent het gebruik van cookies die aan de Internetter verschaft moet worden (zie voetnoot 10) en de specifieke informatie die verstrekt moet worden wanneer reclame per elektronische post wordt gestuurd (zie III.B.3.: Gegevens gebruiken voor direct marketing).

<sup>32</sup> Zie voetnoot 12.

hebben verzet worden gebruikt) zijn een aantal zaken die de onderneming daartoe zou moeten invoeren.

### 1.2.1. Het recht op toegang en verbetering

Behalve een recht op verbetering van zijn persoonsgegevens dat de betrokken persoon kosteloos moet kunnen uitoefenen heeft de persoon die het bewijs van zijn identiteit voorlegt ook een recht op toegang tot de gegevens die op hem betrekking hebben. Op grond van dit laatste heeft hij het recht om van de verantwoordelijke voor de verwerking diverse informatie te verkrijgen over zijn gegevens. Dit recht hoeft niet noodzakelijk kosteloos te zijn<sup>33</sup>. De persoon mag vragen welke gegevens over hem verwerkt worden, aan wie ze worden verstrekt, voor welk doel of welke doeleinden, hij mag vragen om een kopie ervan en alle informatie over de oorsprong ervan te krijgen. De informatie moet onverwijld worden meegedeeld en uiterlijk binnen vijftienvertig dagen na de ontvangst van het verzoek daartoe.

### 1.2.2. Het recht op verzet

Tot slot heeft de persoon het recht zich te verzetten tegen de verwerking van zijn gegevens. Dit recht is kosteloos, en kan zonder opgave van redenen uitgeoefend worden als de gegevens worden gebruikt voor direct marketing. In andere gevallen kan de persoon zich slechts om zwaarwegende en gerechtvaardigde redenen verzetten tegen de verwerking. Er is evenwel geen verzet mogelijk, als de gegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting van de verantwoordelijke voor de verwerking.

## 2. Back Office verplichtingen

### 2.1. Aangifte bij de Commissie voor de bescherming van de persoonlijke levenssfeer

Volgens artikel 17 van de wet van 1992 dient de verantwoordelijke voor de verwerking een aangifte van zijn verwerking te doen bij de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna «de Commissie»). Deze aangifte moet gedaan worden voordat wordt overgegaan tot de verwerking. Dit kan nu elektronisch gebeuren via de website van de Commissie [www.privacy.fgov.be](http://www.privacy.fgov.be). Wel dient men verwerkingen met niet samenhangende doeleinden apart aan te geven (het verzamelen van gegevens voor marketing-

<sup>33</sup> De verantwoordelijke voor de verwerking kan natuurlijk beslissen om dit recht kosteloos te verlenen.

doeleinden en voor veiligheidsredenen dienen b.v. in verschillende aangiften vermeld worden).

In sommige omstandigheden en onder specifieke voorwaarden wordt de verantwoordelijke vrijgesteld van zijn aangifteplicht<sup>34</sup> – zonder echter van zijn andere verplichtingen vrijgesteld te zijn. Worden vrijgesteld de verwerkingen van persoonsgegevens die uitsluitend gebruikt worden voor en/of betrekking hebben op:

- de loonadministratie van het personeel van de verantwoordelijke;
- de administratie van het personeel van de verantwoordelijke;
- de boekhouding van de verantwoordelijke;
- de administratie van aandeelhouders en vennoten;
- het beheer van de klanten of leveranciers van de verantwoordelijke;
- de registratie van bezoekers in het kader van een toegangscontrole.

Worden ook vrijgesteld, de verwerkingen van persoonsgegevens die:

- verricht worden door een stichting, een vereniging of enig andere instelling zonder winstoogmerk in het kader van haar gewone activiteiten (onder bepaalde voorwaarden);
- noodzakelijk zijn voor communicatie die alleen worden verricht om met de betrokken persoon in contact te treden (onder bepaalde voorwaarden);
- verricht worden door onderwijsinstellingen met het oog op het beheer van hun relaties met hun leerlingen of studenten;
- door gemeenten verricht worden overeenkomstig de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, overeenkomstig de kieswetgeving en overeenkomstig de wetsbepalingen inzake de registers van de burgerlijke stand;
- verricht worden door administratieve overheden indien de verwerking is onderworpen aan specifieke door of krachtens de wet uitgevaardigde regelgevingen waarin de raadpleging, het gebruik en de verkrijging van de verwerkte gegevens worden geregeld;
- door instellingen van sociale zekerheid bedoeld in de artikelen 1 en 2, eerste lid, 2° van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid die de toepassing van de sociale zekerheid tot doel hebben, op voorwaarde dat deze instellingen met betrekking tot deze verwerkingen voldoen aan de bepalingen van de vermelde wet en haar uitvoeringsbesluiten.

<sup>34</sup> Zie artikelen 51 tot 62 van 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, B.S. 13 maart 2001.



## 2.2. Algemene beveiligingsverplichtingen van de verantwoordelijke

Een belangrijke bepaling van de Wet van 1992 heeft betrekking op de veiligheidsmaatregelen die door de verantwoordelijke dienen nageleefd te worden<sup>35</sup>.

Concrete maatregelen zijn in de wet niet te vinden. De verantwoordelijke moet zelf nagaan welke beveiliging best past, «rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen, en anderzijds met de aard van de te beveiligen gegevens en de potentiële risico's»<sup>36</sup>. Dit evenwicht is natuurlijk moeilijk op voorhand te beschrijven. Ons inziens moet het algemeen criterium van de *goede huisvader* gebruikt worden om te oordelen of een onderneming aan haar beveiligingsplicht heeft voldaan: *hoe zou iemand, met dezelfde kennis, en in dezelfde omstandigheden de gegevens beveiligen?*

In ieder geval bepaalt de wet dat door de implementatie van deze technische en organisatorische maatregelen moet kunnen worden voorkomen dat de gegevens toevallig of ongeoorloofd vernietigd of gewijzigd worden of verloren gaan. Ook moet erover gewaakt worden dat er geen niet toegelaten verwerking van persoonsgegevens gebeurt. De gegevens moeten juist, up-to-date, ter zake dienend zijn en alléén verwerkt worden door mensen die er de toegang toe en de verwerkingsmogelijkheden voor hebben gekregen.

Verder legt de wet nog algemene verplichtingen op: de verantwoordelijke moet «er nauwlettend over waken dat de gegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens (...) worden verbeterd of verwijderd», en ervoor zorgen dat de personen die de gegevens verwerken, een toegang en verwerkingsmogelijkheden hebben die beperkt zijn «tot hetgeen noodzakelijk is voor de behoeften van de dienst». De verantwoordelijke moet ook «alle personen die onder zijn gezag handelen, kennis geven van de bepalingen van deze wet en haar uitvoeringsbesluiten, alsmede van alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer die bij het verwerken van persoonsgegevens gelden». Tenslotte mag elke persoon die zich onder het gezag van de verantwoordelijke bevindt, en die toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verantwoordelijke verwerken.

Om de Wet van 1992 op dit vlak correct na te leven mogen ondernemingen zich niet beperken tot het implementeren van technische beveiligingsmaatregelen. Firewalls, toegangs- en verwerkingsbeperkingen volstaan hier niet. Er

<sup>35</sup> Met name het artikel 16 van de Wet.

<sup>36</sup> Artikel 16, § 4, Wet van 8 december 1992.

moeten vanzelfsprekend ook organisatorische maatregelen getroffen worden (informereren van de werknemers, interne gedragscode, procedures, enz.).

## 2.3. Verplichtingen indien de verwerking wordt toevertrouwd aan een verwerker.

Indien de verantwoordelijke een verwerking aan een verwerker toevertrouwt, zoals, bijvoorbeeld, het collationeren van gegevens, het updaten van postnummers of het sturen van mailings naar zijn klanten, moet de verantwoordelijke aan verschillende verplichtingen voldoen die betrekking hebben op de beveiliging van de gegevens. De Belgische Wet van 1992 voorziet in boetes van honderd tot twintigduizend<sup>37</sup> euro indien deze verplichting niet nageleefd wordt.

De gekozen verwerker moet voldoende waarborgen bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen die toegepast worden op de verwerking. Deze maatregelen moeten contractueel tussen de verantwoordelijke en diens verwerker vastgelegd worden, samen met de aansprakelijkheid van de verwerker ten aanzien van de verantwoordelijke. De verwerker – en eenieder die handelt onder zijn gezag – mag immers slechts handelen in opdracht van de verantwoordelijke.

Praktisch heeft deze verplichting als gevolg dat, indien een databank met persoonsgegevens gehost wordt door een andere onderneming, voor rekening van de verantwoordelijke, een contract m.b.t. beveiligingsmaatregelen afgesloten moet worden tussen de verantwoordelijke en deze onderneming. Wettelijk gezien draagt de verantwoordelijke alle aansprakelijkheid voor het schenden van de beveiligingsverplichting. Hij zal ook door de aanklagers aangesproken worden. Enkel contractuele afspraken kunnen deze verantwoordelijkheid overdragen op de verwerker.

## IV. CONCLUSIE

Vooraleer gegevens van klanten of prospecten via een website te verzamelen moet elke onderneming zich verschillende vragen stellen die in twee categorieën verdeeld kunnen worden: enerzijds vragen met betrekking tot de toepassing van de wet en anderzijds vragen omtrent de organisatie van de verwerking.

<sup>37</sup> Deze bedragen dienen vermenigvuldigd te worden met vijf en half.

De «toepassingsvragen» die een onderneming zich dient te stellen zijn met name:

- of zij persoonsgegevens verzamelt;
- of zij de verantwoordelijke voor de verwerking is;
- onder welke nationale wet ze valt.

Indien zij, door te antwoorden op deze vragen, tot de conclusie komt dat zij de verantwoordelijke is van een verwerking die onder de Belgische Wet valt, dient ze zich nog af te vragen of ze aan alle wettelijk bepaalde organisatorische en technische maatregelen voldoet. Hiervoor moet ze nagaan of:

- ze de persoonsgegevens wel mag verwerken;
- ze de persoonsgegevens volgens de algemene wettelijke voorwaarden verwerkt;
- ze voldaan heeft aan haar back office-verplichtingen (aangifte verrichten, implementatie van beveiligingsmaatregelen, contractuele afspraak omtrent het verwerken en beveiligen van persoonsgegevens door een verwerker);
- en aan haar front office-verplichtingen (wettelijke informatie verstrekken aan de betrokkene, zijn rechten eerbiedigen).

Het volstaat dus niet een «privacy disclaimer» in te lassen op een Internet website om te voldoen aan alle verplichtingen die voortvloeien uit de Wet tot bescherming van de persoonlijke levenssfeer.

Het naleven van al deze verplichtingen zal zorgen voor het vermijden van door de wet vermelde straffen, zoals boetes (die van 100 tot 100.000 EUR<sup>38</sup> kunnen lopen), controles door de Commissie voor de bescherming van de persoonlijke levenssfeer<sup>39</sup>, veroordelingen tot het uitwissen van de bestanden, of tot het verbod om persoonsgegevens te verwerken gedurende een zekere periode<sup>40</sup>.

Maar het naleven van deze verplichtingen kan ook als een opportuniteit worden beschouwd. De bescherming van het privé-leven en de persoonsgegevens wordt zodanig een bezorgdheid van eenieder dat de eerbiediging van de wet ook de enige mogelijkheid is om het vertrouwen van zijn klanten en prospecten te winnen en te behouden.

<sup>38</sup> Deze bedragen dienen vermenigvuldigd te worden met vijf en half.

<sup>39</sup> De wet voorziet grote controlebevoegdheden voor de Commissie.

<sup>40</sup> Een rechter zou dit verbod tot 2 jaar kunnen opleggen.