Privacybescherming en e-business: (on)verenigbaar ?

Erik Luysterborg
Director, Head of ITEC Group
Deloitte & Touche, Tax & Legal

Vanuit commercieel oogpunt, kan het duidelijk zichtbaar implementeren van een transparante " data privacy "-procedure een krachtig marketing-instrument worden.
Het kan aldus het vertrouwen in de website bij de klant versterken en blijk geven van een bedrijf met een duidelijke visie, bekommerd om de privacy van zijn klanten.

Inleiding

Het onverdeeld optimisme en enthousiasme dat de begindagen van het internettijdperk kenmerkte wordt tegenwoordig regelmatig getemperd door minder uitbundige berichtgeving. Internetbedrijven lijken ook vatbaar voor faillissement en winsten blijken niet altijd even astronomisch als voorspeld.

Hoewel niemand eraan twijfelt dat elektronische handel wel degelijk de toekomst is en enorme groeikansen biedt voor de economie, lijkt de consument nog niet klaar om de e-commerce of elektronische handel voluit te omhelzen. Eén van de redenen daarvan is de onduidelijkheid van het huidige juridische kader daaromtrent. Inderdaad, een aangepast en transparant juridisch kader is in een elektronische omgeving even noodzakelijk als in de off-lineomgeving. Zoals in een vorig nummer van dit tijdschrift reeds door de heer Walrave werd gesteld[1], zijn er op Europees niveau reeds verschillende richtlijnen uitgewerkt die een kader moeten scheppen voor elektronische handel. De belangrijkste voorbeelden daarvan zijn de Europese richtlijn betreffende elektronische handel[2], de Europese richtlijn aangaande elektronische handtekeningen[3] en de richtlijn aangaande de verkoop van goederen op afstand[4].

Een andere reden voor de twijfel van de consument is dat hij zich bij het verstrekken van informatie on line "onveilig" voelt: er lijkt zich bij deze laatste een toenemende bewustwording te ontwikkelen van de gevaren die het internet en in het bijzonder elektronische handel opleveren met betrekking tot de bescherming van privacy.

Consumenten beginnen de mogelijkheden tot misbruik van persoonlijke gegevens op het internet in te zien en meer en meer gaan zij bescherming van die gegevens vooropstellen als voorwaarde tot commercieel gebruik van het internet. De kracht van de technologie om in mensen hun leven binnen te dringen geeft het internet de mogelijkheid om zich als een soort on line "Big Brother" te gaan gedragen die zijn gebruikers non-stop bespioneert voor commerciële of andere doeleinden (bijvoorbeeld door middel van "tracking" middelen zoals de hierna aangehaalde "cookies").

Het is dan ook niet verwonderlijk dat consumenten door dit vooruitzicht niet worden aangesproken. Ze zullen dan ook garanties eisen van diegene die zijn goederen of diensten via het internet aanbiedt dat hun persoonlijke gegevens op de nodige bescherming kunnen rekenen. Ook op het internet is de klant koning en de service (in dit geval de bescherming) die een handelaar biedt kan, net zoals in de off-lineomgeving, de doorslag geven bij het maken van de beslissing om al dan niet via het internet te kopen.

Niet enkel vanuit deze optiek is het voor de ondernemer belangrijk om zijn cliënten dergelijke "service" te bieden, ook de wet legt de ondernemer een aantal verplichtingen op in verband met de verwerking van persoonsgegevens en wel onder de Privacywet van 1992[5].

Deze Privacywet werd in 1998 volledig herzien teneinde de Europese richtlijn van 1995 aangaande de bescherming van persoonsgegevens[6] in het Belgische recht te implementeren. Bovendien staan er nog een aantal uitvoeringsbesluiten op stapel die de toepassing van de vernieuwde wet zullen moeten toelichten. Alhoewel reeds enkele jaren oud, krijgen de bepalingen en verplichtingen daarin vervat pas nu een verhoogde aandacht, enerzijds wegens de toenemende "privacybekommernis" van de consument en anderzijds wegens het nakende einde van de "overgangsperiode" voor de implementatie van de verplichtingen daarin vervat.

De "Europese richtlijn aangaande de bescherming van individuen met betrekking tot de verwerking van persoonsgegevens en de vrije beweging van zulke gegevens" is van kracht sinds 25 oktober 1998 en heeft tot doel binnen de Europese Unie een zeer hoge graad van bescherming van persoonsgegevens te creëren en tevens veiligheidsmaatregelen te voorzien voor transfers van persoonsgegevens buiten de Europese Unie. Alhoewel de richtlijn een ruimere toepassingssfeer ambieert dan het internet, is haar relevantie in de digitale context overduidelijk.

Het is daarom zeker nuttig om de implementering van deze richtlijn in België in de Privacywet van 1992 even te overlopen in een eerste deel van dit artikel. In een tweede deel zal dan een concreet "business-plan" worden voorgesteld dat kan gebruikt worden als leidraad bij het evalueren van de nodige procedures, alsook een idee geeft van de impact van deze reglementering op uw e-commerce-initiatieven.

Belangrijkste principes van Richtlijn 95/46/EC aangaande de bescherming van persoonsgegevens geïmplementeerd in België op 11/12/1998 in de Privacywet van 8 december 1992

Zoals vermeld is de privacywet in 1998 grondig gewijzigd teneinde de Belgische wetgeving in overeenstemming te brengen met de Europese Richtlijn aangaande bescherming van persoonlijke gegevens. De belangrijkste veranderingen die de implementering teweegbracht zijn hierna kort geschetst.

Definities

Zoals bij iedere wettekst is een duidelijk begrip van de gehanteerde definities van primordiaal belang voor het inschatten van de impact van dergelijke wet. Enkele kernbegrippen worden in artikel 1 van deze wet zeer grondig omschreven en bepalen bijgevolg op welke handelingen en personen de regels van de wet van toepassing zullen zijn.

Hierna volgt een kort overzicht van de belangrijkste begrippen:

"Persoonsgegevens" omvatten iedere informatie die betrekking heeft op een identificeerbaar natuurlijk persoon. Deze persoon wordt in de wet de "betrokkene" genoemd en is dus als het ware het onderwerp van de gegevensverwerking.

Het begrip "verwerking" wordt onder impuls van de Europese richtlijn aanzienlijk uitgebreid ten opzichte van de vorige versie van de wet en is *nu duidelijk voorzien op een digitale context.* Verwerking wordt omschreven als "elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens al dan niet uitgevoerd met behulp van geautomatiseerde procédés".[7] Als verduidelijking worden er dan een aantal voorbeelden gegeven die aantonen dat het begrip allesomvattend wordt bedoeld zoals bijvoorbeeld het verzamelen, bewaren, opvragen, vernietigen, gebruiken, ... van dergelijke gegevens.

De "verantwoordelijke voor de verwerking" is diegene in wiens opdracht de gegevensverwerking plaatsvindt en die "het doel en de middelen voor de verwerking van persoonsgegevens bepaalt". Dit kan zowel een natuurlijke persoon als een rechtspersoon zijn en het is deze persoon die zal verantwoordelijk zijn voor de verwerking en derhalve ook instaat voor het naleven van de voorschriften van de wet[8].

De "verantwoordelijke voor de verwerking" moet onderscheiden zijn van de "verwerker van de persoonsgegevens", de natuurlijke persoon of rechtspersoon die in opdracht van de verantwoordelijke de eigenlijke verwerking uitvoert[9]. Dit kan bijvoorbeeld een computerfirma zijn die de gegevensbestanden voor een opdrachtgever beheert en aanpast.

Een laatste begrip dat enige toelichting verdient is "de toestemming van de betrokkene". Hiermee wordt elke "vrije, specifieke, en op informatie berustende wilsuiting verstaan waarmee de betrokkene ... aanvaardt dat persoonsgegevens aangaande de betrokkene worden verwerkt"[10]. *De toestemming van de betrokkene is cruciaal in de vernieuwde wet* en wordt bijvoorbeeld in art. 5 als voorwaarde gesteld voor de verwerking van persoonsgegevens, tenzij in welbepaalde uitzonderingen (bijvoorbeeld indien de verwerking noodzakelijk is voor het uitvoeren van de overeenkomst). De uitzonderingen worden in de wet opgesomd en dienen restrictief te worden geïnterpreteerd (zie verder).

Principes van de persoonlijke gegevensverwerking

Bij het verwerken van persoonlijke gegevens moet de "verantwoordelijke voor de verwerking" zich aan de principes van persoonlijke gegevensverwerking houden die omschreven worden in hoofdstuk twee van de wet. Sommige van deze principes waren reeds aanwezig in de vorige versie van de Privacywet, maar de Richtlijn dwong de Belgische wetgever toch tot een aanzienlijke uitbreiding.

Zo mag men de gegevens enkel en alleen verwerken voor "welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden" [11] en moeten ze bovendien "terzake dienend, toereikend en niet overmatig zijn"[12].

Zij moeten bovendien nauwkeurig zijn, moeten worden aangepast indien nodig en mogen niet langer bewaard worden dan nodig voor de doeleinden van de verwerking.[13]

Belangrijk voor de verwerking van gegevens op het internet is dat de verantwoordelijke voor de verwerking moet voorzien in voldoende technische maatregelen om de verwerking op een confidentiële en veilige manier te laten verlopen en bovendien mag *een transfer van gegevens naar een land buiten de EU enkel gebeuren indien er door dat land voldoende waarborgen worden verschaft voor bescherming van persoonsgegevens* (zogenaamde criterium van "adequate bescherming" onder de in dat land geldende regels). Deze transfers mogen enkel gebeuren indien er aan bepaalde voorwaarden is voldaan [14].

Het is vooral door deze bepaling dat de Richtlijn momenteel weer volop in de belangstelling staat. De Verenigde Staten wordt nog steeds niet beschouwd als een dergelijk land dat "adequate bescherming" biedt in verband met de bescherming van persoonlijke gegevens. Gedurende reeds twee jaar werden verregaande discussies gevoerd tussen de Amerikaanse en EU afgevaardigden om tot een vergelijk te komen die het mogelijk zou maken om persoonsgegevens tussen de twee regio's toe te laten zonder al te grote hindernissen.

In juli jongstleden werden dan de zogenaamde "*Safe Harbour principles*" formeel goedgekeurd. Deze betreffen een overeenkomst tussen de Europese Unie en de Verenigde Staten aangaande het door de Verenigde Staten te waarborgen niveau van bescherming van persoonsgegevens teneinde transfers van gegevens tussen beide regio's mogelijk te maken. Het is gebaseerd op het feit dat Amerikaanse bedrijven vrijwillig zich ertoe verbinden deze "Safe Harbour principles" (vrijwel alle principes vervat in de Europese Privacy Richtlijn) na te leven. De Amerikaanse autoriteiten verbinden zich ertoe op de correcte naleving ervan toe te zien. Dit systeem zou operationeel moeten zijn in november 2000. Alhoewel dit niet betekent dat de Verenigde Staten de status van "adequate bescherming" hebben verkregen, betekent dit toch een doorbraak in de bescherming en uitwisseling van persoonsgegevens tussen de twee

regio's. Financiële diensten zijn hierbij nog niet ingesloten.

Tenslotte dient nog vermeld dat de Europese Commissie op 29 september 2000 onder artikel 26.4 van de Richtlijn een eerste versie heeft gepubliceerd van een modelcontract dat de bescherming van persoonsgegevens bij internationale transfers tussen bedrijven moet regelen.
Het betreft hier de transfers van persoonsgegevens tussen bedrijven gevestigd in de EU en bedrijven gevestigd in landen die niet voorzien in een adequate privacybescherming.

Rechten van de betrokkene

De rechten van de betrokkene bevinden zich in hoofdstuk drie van de gecoördineerde Privacywet en kunnen als volgt worden samengevat.

Allereerst heeft de betrokkene *het recht om geïnformeerd te worden* dat er gegevens aangaande zijn persoon worden verwerkt.
De informatie die aan de betrokkene moet worden meegedeeld betreft hoofdzakelijk de identiteit van de verantwoordelijke voor de verwerking en de doeleinden van de verwerking[15].

Betrokkene moet ook gewezen worden op zijn *recht op toegang tot en verbetering van de op hem betrekking hebbende gegevens.* Het recht op toegang wordt geregeld door artikel 10 van de wet en houdt in dat de verantwoordelijke voor de verwerking op eerste verzoek van de betrokkene deze laatste moet voorzien van alle gegevens die verwerkt worden alsook de bron waar de gegevens vandaan komen. Dit alles dient volbracht te worden binnen een redelijke termijn.

Daarenboven geeft artikel 12 de betrokkene *het recht om onjuiste persoonsgegevens die betrekking hebben op hem kosteloos te doen verbeteren.* In uitzonderlijke gevallen heeft betrokkene zelfs het recht om zich te verzetten tegen de verwerking "in se". Wanneer de verwerking gebeurt voor doeleinden van "direct marketing" heeft betrokkene steeds het recht zich te verzetten tegen de verwerking.

Deze regels zullen een belangrijke invloed hebben op de interne organisatie en controle van een onderneming en dit zowel aangaande haar on-line- als off-line-activiteiten.

Verplichtingen van de verantwoordelijke voor de verwerking

Allereerst moet de verantwoordelijke voor de verwerking erop toezien dat hij de rechten van de betrokkene zoals hierboven beschreven niet schendt.

De tweede belangrijke categorie van verplichtingen heeft betrekking op het principe van geheimhouding en beveiliging van de verwerking. Hoofdstuk vier van de gecoördineerde Privacywet legt hieromtrent de verplichtingen van de verantwoordelijke van de verwerking vast. Een voorbeeld van deze verplichtingen is dat de verantwoordelijke voor de verwerking een verwerker moet kiezen die *voldoende technische en organisatorische beveiligingsmaatregelen* voorziet *voor de verwerking van de gegevens*[16]. Dit zal een belangrijke invloed hebben op de contractuele relatie tussen de onderneming en derde partijen (bijv. Website hosts/ Data centers etc.)

De belangrijkste verplichting van de verantwoordelijke voor de verwerking is dat hij voorafgaand aan de verwerking van persoonsgegevens hiervan *aangifte* moet doen *bij de Commissie voor de bescherming van de persoonlijke levenssfeer.*
De regels hieromtrent worden vastgelegd in hoofdstuk vijf van de gecoördineerde Privacywet.
De belangrijkste gegevens die de aangifte moet bevatten hebben betrekking op de identiteit van de verantwoordelijke voor de verwerking, het doel van de verwerking, en de categorieën van personen aan wie de gegevens zullen worden meegedeeld (art. 17§3).
De aangifte moet bijkomende gegevens bevatten indien bepaalde gegevens bestemd zijn voor doorzending naar het buitenland.[17]

Gevallen waarin persoonsgegevens mogen worden verwerkt

Buiten de algemene principes, de rechten van de betrokkene en de verplichtingen van de verantwoordelijke voor de verwerking is het nog belangrijk om art.5 en art. 6 te vermelden aangezien deze een belangrijke impact kunnen hebben op de wijze waarop gegevens op het internet worden verzameld.

- Art. 5 bepaalt namelijk *een gelimiteerd aantal gevallen waarin gegevensverwerking is toegelaten.*
  De belangrijkste gevallen zijn:
  - wanneer de betrokkene zijn uitdrukkelijke toestemming geeft;
  - wanneer de verwerking noodzakelijk is voor de uitvoering van een contract waarbij de betrokkene partij is;
  - wanneer de verwerking van vitaal belang is voor de betrokkene;
  - wanneer de verwerking noodzakelijk is om een wettelijke verplichting na te komen.

Dit wil zeggen dat wanneer de verwerking niet essentieel noodzakelijk is voor de uitvoering van een contract, de uitdrukkelijke toestemming van de betrokkene bijna altijd zal vereist zijn. Dit heeft zoals ik verder zal zien belangrijke consequenties, bijvoorbeeld bij het plaatsen van "cookies".

Bovendien behandelt art.6 *de verwerking van gevoelige gegevens zoals gegevens rond raciale of etnische afkomst of politieke overtuiging,* die in principe steeds verboden is tenzij men uitdrukkelijke toestemming verkrijgt van de betrokkene. Ook dit dient in een internetcontext extra aandacht te krijgen.

De Privacywet en haar impact op de onderneming

Inleiding

Niettegenstaande het ontbreken van een uitvoeringsbesluit voor de wet van 11 december 1998, zal de onderneming met een *aantal ingrijpende veranderingen* geconfronteerd worden. Zowel interne als externe verwerking en transmissie van gegevens kunnen de Belgische bedrijven problemen bezorgen, wanneer het er op aan komt zich aan te passen aan de nieuwe wetgeving.
Verschillende punten trekken de aandacht.

Naar de buitenwereld toe zijn er *drie verschillende fronten waar men waakzaam dient te zijn* betreffende de bescherming van de persoonsgegevens.

Naar de klant toe betreft dit vooral het feit of het bedrijf zijn toestemming op een duidelijke en expliciete manier heeft verkregen (bijvoorbeeld door een geschrift of door het klikken op de website) tot het opslaan en de verwerking van de gegevens. Een tweede aspect betreft het feit of het bedrijf de klant op

voldoende wijze heeft ingelicht (in het contract of op de website) over de wijze van opslaan en de plaats en doel van de verwerking van zijn persoonlijke gegevens.

Naar derde partijen toe (bijvoorbeeld een leverancier), moet men erop letten of er voldoende contractuele waarborgen zijn bedongen tot bescherming van de persoonsgegevens.

Tenslotte is er ook nog *de relatie met de overheid* (zie boven), die in bepaalde gevallen door het bedrijf uitvoerig moet worden ingelicht betreffende de redenen van en de omstandigheden waarin persoonsgegevens van werknemers en klanten worden opgeslaan en verwerkt. Diezelfde overheid heeft dan ook toezichthoudende bevoegdheden.

Binnen het bedrijf moet vooral de bescherming van de persoonlijke gegevens van de werknemers worden beoogd, in correlatie met het uitwerken van een duidelijke structuur voor de toegang tot deze gegevens. Naast de bescherming ervan, dient ook nagegaan te worden of deze gegevens overeenstemmen met de wettelijke voorschriften (bijvoorbeeld CAO's). Eveneens is het van belang een duidelijk overzicht te hebben van alle « flows » van persoonsgegevens binnen en tussen de verschillende afdelingen (en filialen) van het bedrijf. Hierna worden kort een aantal van de belangrijkste aandachtspunten besproken.

Multidisciplinaire aanpak

Om zowel intern als extern de beoogde bescherming te kunnen waarborgen, lijkt het aangewezen vanuit een algemene aanpak te vertrekken.

Het komt er vooreerst op aan een klare kijk te krijgen op uw huidige bedrijfscultuur inzake het bewaren en de transmissie van persoonlijke gegevens. Waar worden de gegevens bewaard, door wie worden ze verwerkt, wie is de verantwoordelijke, zijn de gegevens gemakkelijk toegankelijk, door wie zijn ze toegankelijk, vindt er transmissie van gegevens plaats, binnen België, binnen Europa of daarbuiten,...?

Op al deze vragen dient een afdoend antwoord te worden geformuleerd. Om dat te bereiken is het noodzakelijk een multidisciplinaire « task force » te creëren.
Bescherming van persoonsgegevens is niet een louter IT-gebeuren, het heeft belangrijke juridische, marketing en organisatorische implicaties.

Verantwoordelijke en structuur van de organisatie

Zoals reeds eerder vermeld dient men een verantwoordelijke voor de bescherming van de persoonlijke gegevens aan te duiden, aan wie het toekomt zich perfect te informeren inzake intern en extern beheer van gegevens. Het spreekt vanzelf dat deze persoon daarvoor voldoende op de hoogte dient te zijn van de internet-/intranetstrategie van het bedrijf en van de wettelijke verplichtingen en verantwoordelijkheden, die dienaangaand op het bedrijf en op hem/haar rusten. In de praktijk laat de interne communicatie tussen de verschillende departementen in veel gevallen echter te wensen over: ze is ofwel niet bestaand, gebrekkig of levert tegenstrijdige informatie op.

Interne "flow"

Het geheel van « intern » verkeer van gegevens gaat verder dan men op het eerste zicht zou vermoeden. Uitgaande van een klantenbestand bijvoorbeeld, ziet men dat dit bestand niet alleen circuleert binnen het marketingdepartement, maar dat dit bestand ook kan gebruikt worden door een buitenlandse afdeling van het bedrijf. Nog andere departementen kunnen mogelijks gebruik maken van persoonsgegevens, zoals de human resources (rekruteringsdoeleinden) of de distributiekanalen (levering van producten) en de administratie (facturatie, opmaken van contracten). Naargelang de aard en structuur van de organisatie en herkomst van de gegevens, kan de tussenkomende partij dus van verschillende aard zijn.

Binnen het bedrijf of de organisatie is het dan ook belangrijk te weten of het personeel dat met persoonlijke gegevens in aanraking komt, voldoende opgeleid werd in deze materie en of er regels voor toegang tot de databases bestaan (hoe deze opgevolgd worden en hoe ze afgedwongen worden ?).

Tot slot, maar daarom niet minder belangrijk, dringen er zich ook verschillende interne technische veiligheidsmaatregelen op.
Verscheidene vragen werpen zich hier op aan het adres van het bedrijf: werd er informatie opgeslagen in servers die toegankelijk zijn via het internet, zijn de servers goed beveiligd, hoe verloopt de toegang tot deze servers?

Het is dus van belang niet alleen op papier, maar ook daadwerkelijk binnen de organisatie een privacy « awareness » te creëren. Dit kunt u alleen maar verkrijgen worden door regelmatige training en voorlichting.

Externe "flow"

Als men het externe verkeer van gegevens bekijkt, zeker in de e-businesscontext, dan merken we het groot aantal derde tussenpersonen ». Zoals derden die bepaalde taken voor het bedrijf verzorgen (koerierdiensten, onderhoud van de informaticastructuur), Internet hosting providers, wettelijke instanties (RSZ, BBI), banken, call centers, en dergelijke. De verantwoordelijke moet dus beide, intern en extern verkeer, beheersen teneinde zijn taak volwaardig te kunnen vervullen.
Wederom verschillen de tussenkomende partijen naargelang de aard van de activiteit en de noden van het bedrijf. Een sluitend contractueel kader alsook de nodige controlemogelijkheden dringen zich op.

Toestemming van de betrokken persoon

Naar de betrokken persoon toe, en vooral wat betreft het verkrijgen van een onmiskenbare toestemming voor het gebruik van zijn gegevens voor bepaalde doeleinden, stelt zich de vraag of deze toestemming uitdrukkelijk en ten bijzondere titel werd verkregen. Werd er expliciet vermeld dat de gegevens bestemd waren voor direct marketing of transmissie aan derde partijen, eventueel buiten de Europese Unie ? Werd de toestemming verkregen voor het gebruik van vertrouwelijke gegevens ? In dit opzicht willen we ook verwijzen naar het principe van de 'Tick box' (dit is het icoon op het scherm, dat, door middel van een simpele klik, de persoon toelaat zich akkoord te verklaren met algemene voorwaarden, gebruik van zijn gegevens voor bepaalde doeleinden). Dergelijke praktijk wordt doorgaans aanvaard mits het verstrekken van nadere, voorafgaande uitleg aan de consument waaruit ontegensprekelijk de gevolgen van een dergelijke klik blijken. Dit betekent dat de structuur van uw website een belangrijke rol zal spelen voor

het beoordelen van de juridische gevolgen.

Het verkrijgen van de toestemming van de betrokkene (en het daaraan verbonden recht op inzage en verbetering) vormt een cruciaal onderdeel in de aanpassing van de organisatie aan de vereisten van nieuwe wetgeving.

Marketing en cookies

Met betrekking tot de toestemming van de betrokken persoon, past het, zij het kort, het thema van de cookies aan te snijden. Men kan ze beschrijven als kleine bestanden, die een uniek referentienummer bevatten en opgeslagen worden op de harde schijf van de computer van de internet gebruiker/bezoeker, wanneer deze gebruiker een bepaalde website bezoekt. Als men een site bezoekt dan kan de server, waar deze site opgeslagen is, naar het navigatieprogramma van de computer een of verschillende van deze bestanden zenden. Iedere keer dat je naar dezelfde server gaat, zal deze cookie zich opnieuw melden en de server toelaten je sporen op de website te volgen.

Door de gewoontes te kennen, te weten welke sites de klant bezoekt en welke informatie hij opvraagt, wordt de server van het bedrijf in de mogelijkheid gesteld om de volgende keer, direct op maat gemaakte informatie door te sturen naar de klant (one-to-one marketing door middel van bijvoorbeeld gepersonaliseerde boodschappen of reclame). Dit is een belangrijk instrument voor het bedrijf, maar in werkelijkheid kunnen de cookies ertoe bijdragen om een persoon te identificeren (in dit geval vallen ze onder de bescherming van de wet van de bescherming van de persoonsgegevens) en bepaalde gevoelige gegevens af te leiden uit de bijeengesprokkelde informatie. Het bedrijf hoedt er zich dus beter voor de regels te respecteren teneinde geen inbreuken te plegen op de wet van 11 december 1998. Afhankelijk van het land bestaan er specifieke regels aangaande de informatie die moet gegeven worden aan de consument over het gebruik van dergelijke cookies alsook de mogelijkheden om deze te neutraliseren of te weigeren.

Conclusie

Privacy krijgt zowel juridisch als commercieel meer en meer aandacht. Zoals reeds eerder aangehaald, werd er op Europees vlak een juridisch kader geschapen, waarvan de Belgische wet van 11 december 1998 de nationale implementatie belichaamt. De voornaamste krachtpunten die men kan onthouden, zijn de uitgebreide rechten van de betrokkene in verband met de toegang en wijziging van zijn persoonsgegevens en de verruimde verplichtingen van de verantwoordelijke voor de verwerking en bescherming ervan, in het bijzonder met betrekking tot de transmissie naar niet-EU landen. In praktijk zal de nieuwe wetgeving echter nog voor de nodige implementatie- en aanpassingsproblemen zorgen voor de bedrijven.

De implementatie van de opgelegde verplichtingen dienen niet echter als louter negatief of belas-

tend te worden beschouwd. Vanuit commercieel oogpunt, kan het duidelijk zichtbaar implementeren van een transparante data privacy-procedure echter een krachtig marketinginstrument worden. Het kan aldus het vertrouwen in de website bij de klant versterken en blijk geven van een bedrijf met een duidelijke visie, bekommerd om de privacy van zijn klanten. Men heeft er dus alle belang bij om de implementatie van de nieuwe regels doorheen alle geledingen van het bedrijf kenbaar te maken.

Het voorafgaande toont ook duidelijk aan dat de privacybescherming meer dan ooit een belangrijke plaats inneemt in de verdere succesvolle ontwikkeling van de elektronische handel, voornamelijk dan in de « business-to-consumer » omgeving. Met de toenemende verspreiding van de nieuwe technologieën zal het onderwerp dan ook meer en meer in de spotlight komen te staan.

1 Walrave, P., *E-commerce : een juridische stand van zaken*, West-Vlaanderen Werkz, I, 2000, p.6

2 Richtlijn 2000/31/EG van het Europese Parlement en de Raad van 8 juni 2000 aangaande bepaalde wettelijke aspecten van de informatie maatschappij, in het bijzonder elektronische handel, in de interne markt, *Official Journal*, L178, 17.07.2000.

3 Richtlijn 1999/93/EG van het Europese Parlement en de Raad van 13 december 1999 aangaande een gemeenschapskader voor elektronische handtekeningen, *Official Journal*, L 13, 19.01.2000

4 Richtlijn 97/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten.

5 Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Gecoördineerde versie, zoals laatst gewijzigd door de wet van 11 december 1998, *B.S.*, 3 februari 1999.)

6 Richtlijn 95/46/CE aangaande de bescherming van individuen met betrekking tot de verwerking van persoonsgegevens en de vrije beweging van zulke gegevens.

7 art. 1 §2

8 art. 1 § 4

9 art.1 § 5

10 art.1 § 8

11 art. 4 §1, 2°

12 art. 4 §1, 3°

13 art. 4 §1, 4° & 5°

14 dit is het laatste principe onder in richtlijn 95/46/CE maar wordt in de Belgische wet niet in hoofdstuk twee maar in hoofdstuk zes verder uitgewerkt.

15 art. 9 §1

16 art. 16 §1, 1°

17 art. 16 §6