

verschenen als voorpagina-artikel in Job in de Regio edities 29 augustus 2003 (Rijn-, Gouwen Veenstreek) en 5 september 2003 (Haaglanden; Kust, Duin- & Bollenstreek en Haarlem)

De grenzen van de privacy

Wat gebeurt er met uw persoonsgegevens?

door: Gabor Mooij

Klanteninformatie is geld waard en tegenwoordig beschikken organisaties over meer mogelijkheden dan ooit om aan die informatie te komen. De controle op dat informatie inwinnen is via de Wet Bescherming Persoonsgegevens ook groter dan ooit. Toch weten de meeste mensen niet hoe actief bedrijven zijn in het verzamelen van informatie over hen. De gegevens van een 'gemiddelde' burger komen in honderden bestanden voor. Vaak gaan bedrijven daar netjes mee om. Er zijn er echter ook die het minder nauw met de regels nemen. De overheid, die eigenlijk een voorloper moet zijn op het gebied van het beheren van persoonsgegevens, blijkt in veel gevallen juist een achterblijver te zijn. De burger tenslotte weet vaak niet dat hij of zij recht heeft om de gegevens die een bedrijf over hem of haar bewaart, in te zien en zondig te laten corrigeren.

Bescherming persoonsgegevens

Persoonsgegevens zijn alle gegevens, die iets over een persoon zeggen of die van invloed kunnen zijn op de beoordeling of behandeling van iemand. Naast iemands naam, geboortedatum en adres kan het bijvoorbeeld ook gaan om diens banksaldo, beroep of een kenteknummer. Ook gegevens met een waardering over een individu, bijvoorbeeld diens intelligentiequotiënt (IQ), zijn persoonsgegevens.

Op alle mogelijke manieren kunnen persoonsgegevens door organisaties worden vastgelegd. Voorbeeld zijn de klantenkaart in de supermarkt, het aanmeldingsformulier op het internet of het telefoontje waarin enkele minuten van je tijd wordt gevraagd om wat vragen te beantwoorden. Meestal gebeurt dit netjes door iemand te informeren wat er met de gegevens gebeurt. Ook minder nette praktijken, waarbij iemands gegevens zonder diens toestemming worden verzameld, gebruikt of zelfs verhandeld, komen helaas voor.

Om dit laatste tegen te gaan, is in 2001 de Wet Bescherming Persoonsgegevens (WBP) van kracht geworden. In deze wet zijn de rechten en plichten op het gebied van de omgang met persoonsgegevens omschreven. Naast de WBP zijn er nog andere wetten op het gebied van privacy van kracht. De Telecommunicatiewet bijvoorbeeld regelt wanneer de overheid het internetverkeer van burgers mag aftappen.

De in 2000 opgerichte privacy- en burgerrechtenorganisatie Bits of Freedom komt op voor de rechten op het gebied van auteursrecht, de balans tussen opsporing en privacy, vrijheid van meningsuiting en spam. Sjoera Nas van Bits of Freedom: "In principe dekt de WBP de bescherming van persoonsgegevens goed af. Als de nieuwe Europese richtlijn 'Privacy in de telecomsector' uit 2002 erin wordt verwerkt, is de wet helemaal afdoende. Deze richtlijn bevat namelijk een regeling tegen spam, ongewenste reclame waarmee mensen via de email worden lastiggevallen."

Bij de invoering van de Wet Bescherming Persoonsgegevens is ook het College Bescherming Persoonsgegevens (CBP) opgericht. Dit College verving de Registratiekamer, tot 2001 de privacybeschermer in Nederland.

Het CBP is een onafhankelijke organisatie, die toeziet op een zorgvuldige omgang met persoonsgegevens. Bedrijven zijn verplicht hier het gebruik van persoonsgegevens te melden. Informatie over sollicitanten, uitzendkrachten of personeel is hiervan vrijgesteld. Vaak is de vrijstelling zo moeilijk te bepalen dat een onderneming er verstandig aan doet het gebruik van persoonsgegevens gewoon te melden. Het CBP is namelijk bevoegd een, vaak forse, boete op te leggen als een organisatie de verwerking van persoonsgegevens niet, onjuist of te laat heeft opgegeven.

Daarnaast adviseert het CBP de regering en ook de Raad van Europa over aanpassingen van wet- en regelgeving op het gebied van persoonsgegevens.

Het College mag een organisatie een dwangsom opleggen bij verkeerd gebruik van persoonsgegevens. De overtredende organisatie moet dan binnen een termijn dat gebruik terugdraaien anders moet ze een boete betalen. “De eerste twee jaar van ons bestaan hebben we vooral besteed aan voorlichting en onderzoek. We hebben nu net voor het eerst een dwangsom opgelegd aan een handelsinformatiebureau”, vertelt Barbara den Uijl, voorlichter van het CBP.

Volgens Den Uijl is het toezicht op het gebruik van persoonsgegevens door het CBP een succes. “We hebben al 20 000 meldingen ontvangen. Bij de start van de Wet Bescherming Persoonsgegevens gingen we van in totaal 25 000 meldingen uit voor de tijd dat de wet van kracht is. Het is overigens niet zo dat de WBP maar voor een bepaalde tijd geldt; die 25 000 meldingen zijn puur een schatting wat er aan meldingen bij deze wet in totaal kan binnenkomen. Daarnaast zitten onze telefonische spreekuren 's ochtends, altijd vol.”

Rechten

De Wet bescherming persoonsgegevens geeft de burger uitgebreide mogelijkheden om voor zijn privacyrechten op te komen. Zo kan hij een organisatie vragen welke gegevens deze over hem heeft. Hij mag de gegevens inzien die een bedrijf of instelling over hem heeft. Bij foutieve registratie kan de klant altijd correctie van de gegevens eisen. Verder moet een bedrijf kunnen aangeven waarom ze iemand als klant weigert.

Een klant mag verzet aantekenen bij een organisatie tegen de verwerking van zijn of haar gegevens. Deze organisatie moet hier mee stoppen als dit verzet gerechtvaardigd is en als het belang van de burger zwaarder weegt dan het belang van de gegevensverwerker. Worden de organisatie en de klant het hier niet over eens dan kunnen ze hun geschil voorleggen aan het College Bescherming Persoonsgegevens. Ook kan de klant de rechter inschakelen en om een schadevergoeding vragen. Den Uijl: “Bedrijven en klanten leggen veel van hun geschillen voor aan het CBP. De meeste daarvan gaan niet door naar de rechter”.

Ook mag de consument van een bedrijf dat zijn of haar persoonsgegevens gebruikt om hem of haar te benaderen, eisen dat dit hier direct mee stopt.

Ewald van Kouwen, woordvoerder van de Consumentenbond: “We krijgen weinig klachten van consumenten dat ze zich aangetast voelen in hun privacy. De meeste mensen hebben dat niet door. Als ze gerichte reclame toegezonden krijgen, beseffen ze vaak niet dat dat alleen mogelijk is, omdat een bedrijf gegevens over ze heeft. Ook zijn de consumenten niet altijd goed op de hoogte van de mogelijkheden die ze hebben om hun gegevens te beschermen. De voorlichting daarover is beperkt geweest.”

Nas is het daarmee eens: “De mensen zijn zich onvoldoende bewust van hun rechten op privacygebied. Je merkt ook dat mensen pas bij problemen geïnteresseerd raken in hun privacyrechten. Alleen als klanten massaal gebruik maken van hun rechten, zullen bedrijven er meer rekening mee gaan houden.”

Plichten

Organisaties mogen persoonsgegevens alleen verzamelen en gebruiken voor een duidelijk omschreven doel en om een goede reden. Een goede reden voor het verzamelen en gebruiken van persoonsgegevens is bijvoorbeeld een wettelijke verplichting. Ook kan de verwerking van persoonsgegevens nodig zijn voor bijvoorbeeld het afwickelen van abonnementen, lidmaatschappen en koop- en huurovereenkomsten. Daarnaast kan een organisatie haar activiteiten soms niet goed uitoefenen zonder het gebruiken van persoonsgegevens.

Voor alle bedrijven en instanties die persoonsgegevens verwerken, geldt een informatieplicht. Dit betekent dat zij de personen van wie ze gegevens willen gebruiken, daarover informeren en aangeven wat er met die gegevens gebeurt. Deze informatieplicht geldt niet als de organisatie de gegevens verzamelt of gebruikt op basis van een wettelijke plicht.

Het is verplicht voor bedrijven en overheden persoonsgegevens geheim te houden voor onbevoegden. Ook zijn ze verplicht hun klantgegevens voldoende te beveiligen. Het is al eens gebeurd dat door een lek op de website van een verzekeringsmaatschappij gegevens van klanten zomaar op straat kwamen te liggen. Niet alleen namen, adressen en polisnummers werden openbaar, ook het soort verzekeringen dat klanten hadden lopen bij de verzekeraar.

Toezicht

“Het CBP houdt op twee manieren toezicht op het gebruik van persoonsgegevens”, zegt Den Uijl. “Ten eerste gebruiken we de klachten van particulieren om een organisatie te benaderen met een brief. Als er dan geen duidelijkheid ontstaat, sturen we een tweede brief. Daarna kunnen we eventueel onaangekondigd langsgaan bij het bedrijf of de instantie om ter plekke te controleren. Op de tweede plaats kunnen we het idee krijgen dat er iets niet klopt, dan gaan we zelf op onderzoek uit.”

Nas: “Het CBP beschikt niet over de middelen om voortdurend te controleren.

Ze hebben dan ook voor een zelfcorrigerende aanpak gekozen, waarbij bedrijven een privacyfunctionaris kunnen aanstellen die de omgang met privacy bewaakt.”

Deze onafhankelijk privacyfunctionaris is tegen ontslag beschermd en houdt toezicht op naleving van de privacyvoorschriften door een bedrijf of instantie. Het College Bescherming Persoonsgegevens heeft toegezegd bij bedrijven met een privacyfunctionaris terughoudend te zijn met toezicht.

“Vaak worden databases beheerd door technische mensen van de ICT-afdeling. Die hebben de neiging gegevens te lang te bewaren. De privacyfunctionaris of een privacymedewerker van het bedrijf zelf zou in dat soort gevallen kunnen zorgen voor het binnen de juiste termijn verwijderen van klantgegevens”, zegt Nas.

Achterstanden

Uit een onderzoek van het College Bescherming Persoonsgegevens in januari en april 2003 bleken bepaalde branches achter te lopen met de meldingen van het gebruik van persoonsgegevens.

Den Uijl: “Bedrijven melden over het algemeen het gebruik van persoonsgegevens op tijd. Daar zijn we voorzichtig optimistisch over. Organisaties houden steeds meer rekening met privacy. Er zijn echter sectoren die achterlopen: de overheid, de handels- en informatiebranche, de zorgsector en de marketingbranche. Opvallend is dat de overheid, die eigenlijk een voorttrekkersrol zou moeten vervullen, zo achterblijft. Het gaat daarbij vooral om de gemeenten. We hebben deze hierover aangeschreven in mei en kijken in het najaar wat we hier verder aan doen.”

Internetprivacy

Door de ontwikkeling van het internet is vaak niet meer te volgen wat de technologie met de privacy van de internetter doet. De consument heeft hier ook te weinig kennis van de informatica voor.

Gelukkig is op hetzelfde internet veel informatie te vinden hoe de consument zijn internetgedrag zo veilig mogelijk kan maken.

Het probleem is dat het vrij gemakkelijk is om ongevraagd informatie van iemands PC te halen. Een berucht voorbeeld zijn muziekdownloadprogramma's, zoals Kazaa. Hierin zit software verborgen, die ongevraagd informatie over het internetgedrag van de gebruiker verstuurt naar marketingbedrijven. Gelukkig bestaat er software die dat gespioneer kan tegengaan.

Het massale gratis downloaden van muziek op het internet leidt er daarnaast toe dat de muziekindustrie probeert aan de persoonsgegevens van de downloaders te komen.

“Belangenbehartigers van de muziekindustrie proberen via de rechter internetaanbieders te dwingen klantgegevens af te staan”, vertelt Sjoera Nas. “Die klanten willen ze dan aanklagen voor illegaal gebruik van muziekbestanden. Dit is al een aantal keer in de VS gebeurd en laatst is in Denemarken een eerste rechtszaak tegen een internetaanbieder door de muziekindustrie gewonnen. De internetaanbieder moest toen klantgegevens afstaan. Het is twijfelachtig of deze praktijk op grote schaal gangbaar wordt. Er wordt ongevraagd gebruik gemaakt van iemands adresgegevens, die deze niet voor die doeleinden heeft afgestaan.”

De grootste irritatiefactor voor de internetconsument is echter de spam.

Nas: "In Europa en de VS wordt de spam al vrij effectief aan banden gelegd. Problemen komen vooral uit landen zoals China, waar de spam minder wordt tegengegaan. Hierdoor kan spam uit zo'n land ons toch via het internet en de email bereiken."

Uit onderzoek blijkt dat de meeste consumenten de privacyvoorwaarden op websites niet of nauwelijks lezen. Ook de bedrijven blijken vaak slecht op de hoogte van hun privacyvoorwaarden. Dit blijkt uit een in 2002 gepubliceerd rapport van Jupiter Media Metrix, een Amerikaans bedrijf gespecialiseerd in het internetgedrag van consumenten en bedrijven. Rob Leathern, analist bij Jupiter, verbaast zich erover dat bij veel bedrijven de voorwaarden worden opgesteld door een juridische afdeling, zonder dat deze hierover overleg heeft met de IT-afdeling.

Cowboypraktijken

Uit onderzoek van het CBP bleek dat handelsinformatiebureaus bij veel bedrijven en overheidsinstellingen gemakkelijk aan persoonsgegevens kunnen komen. Dit was zelfs het geval bij organisaties met een wettelijke plicht tot geheimhouding. Eén bureau overtrad de regels zodanig dat het College het een dwangsom oplegde als het niet binnen twee maanden schoon schip zou maken. De branchevereniging van handelsinformatiebureaus werkt inmiddels met het CBP aan een gedragscode. Het betreffende bureau is overigens geen lid van de branchevereniging.

"Bedrijfjes zoals het bureau dat de dwangsom kreeg opgelegd zijn vaak detectivebureautjes, die oplichting niet schuwen om aan persoonsgegevens te komen", zegt Nas. "Zo zijn er meer voorbeelden van cowboypraktijken. Een voorbeeld is dat van consumenten die na het versturen van een SMS-bericht ongewenst vast kwamen te zitten aan een duur abonnement op een SMS-service. Nadat consumentenprogramma's zoals Kassa en Radar hier aandacht aan schonken, werd vanuit de telecombranche actie ondernomen om een einde aan deze praktijken te maken."

Kouwen van de Consumentenbond: "Uiteindelijk weten we niet precies wat er met iemands persoonsgegevens gebeurt. Je kunt nou eenmaal niet achter de schermen van al die organisaties kijken. De consument staat op heel veel plaatsen geregistreerd, veel meer dan hij of zij zelf weet. Er zijn veel nette bedrijven, maar ook bedrijven die het niet zo nauw nemen met iemands gegevens. Nette bedrijven maken duidelijk aan de consument kenbaar hoe ze met diens gegevens omgaan. Overigens is het soms ook gewoon handig voor de consument als een bedrijf goed weet wat diens wensen zijn."