

Is de klant koning (van zijn gegevens)?

Over klantkaarten, Knowledge Discovery in Databases en privacy¹

Mw. mr. E. Wiersema

Knowledge Discovery in Databases wordt langzamerhand gemeengoed. Hierdoor komen vragen over privacy steeds duidelijker naar voren. Een juist begrip van de do's en don'ts kan ervoor zorgen dat privacymissers door KDD worden voorkomen.

1) Dit artikel vormt een bewerking van de scriptie van M.A.J. van der Linden, *Onbekend versus onbe-mind, een profiel van de Wbp*, aan de rechtenfaculteit Universiteit Leiden, geschreven tijdens een stage bij KMPG EDP Auditors/Jurist.

2) P.H.A. Frissen in IT & Recht, april 1998.

Inleiding

Steeds meer ondernemingen willen onder het mom van 'de klant is koning' (bestaande en nieuwe) klanten aan zich binden. Dit wilden en deden ze natuurlijk altijd al, bijvoorbeeld door het uitgeven van spaarzegeltjes of door 'gewoon' een persoonlijke band met de klant te onderhouden. Technische ontwikkelingen in informatietechnologie (IT) bieden echter nieuwe mogelijkheden. Een aantal ondernemingen, met name in de retailsector, geeft reeds klantkaarten uit. Het bekendste voorbeeld daarvan is wel de Bonuskaart van Albert Heijn. Meestal zijn deze klantkaarten gekoppeld aan bepaalde voordelen zoals kortingen op producten en/of diensten. Hiermee worden echter niet altijd de door de onderneming gewilde klanten binnengehaald. Door uit te gaan van de persoonlijke behoefte van de klant, kan de onderneming die klanten aan zich binden die zij ook daadwerkelijk wil hebben.

Om de juiste klanten aan een onderneming te binden, zijn gegevens nodig. Een bedrijf moet weten wat de klant wil voor het geïndividualiseerde aanbiedingen kan doen. Een goed overzicht van het klantenbestand is onontbeerlijk. Het hebben van veel (persoons)gegevens levert echter niet altijd de juiste informatie op om een klantenprofiel samen te stellen. Ten eerste moeten de bestanden met gegevens betrouwbaar, actueel en toegankelijk zijn. Ten tweede zal de enorme hoeveelheid aan gegevens geanalyseerd moeten worden, alvorens deze juist te kunnen interpreteren.

Hier doet Knowledge Discovery in Databases (KDD), ook wel aangeduid met datamining, zijn intrede. KDD wordt gezien als een verfijning van de reeds bestaande analysetechnieken, die vooral mogelijk is gemaakt door de vooruitgang in de techniek. KDD biedt nieuwe mogelijkheden voor klantenbinding. Door KDD zijn organisaties (ondernemingen én overheid) beter in staat een persoon uit een bepaalde doelgroep individueel te benaderen en de persoon wellicht dusdanig te beïnvloeden dat hij het voor de organisatie gewenste gedrag gaat vertonen. Dit brengt echter tegelijkertijd een (groter) risico van privacyschending met zich mee. Weet de klant wat er met zijn gegevens gebeurt?

Mag een bedrijf 'zomaar' het gedrag van klanten met behulp van KDD analyseren en vervolgens gebruiken in

de omgang met de klant(gegevens)? Met andere woorden, is de klant ook nog koning indien het om zijn of haar gegevens gaat? Hierna zal vanuit een juridisch oogpunt worden ingegaan op deze vraag. Nagegaan wordt of de privacywet en/of -regelgeving en in het bijzonder het voorstel Wet bescherming persoonsgegevens van toepassing is op KDD-processen en zo ja, hoe de wet het gebruik van KDD (en het gebruik van klantkaarten) normmeert. Alvorens hierop in te gaan, wordt kort stilgestaan bij het begrip privacy. Waar hebben we het nu eigenlijk over als het om privacy gaat?

Privacy

Privacy wordt over het algemeen pas relevant wanneer een inbreuk daarop dreigt. Daardoor wordt privacy niet direct als een probleem ervaren en wordt het onderwerp in bijvoorbeeld projecten op het gebied van electronic commerce, datawarehousing en/of -mining vaak naar de achtergrond geschoven of er wordt helemaal geen aandacht aan besteed. Het heeft een enigszins zeurderig imago. Dit wordt treffend geïllustreerd door de volgende uitspraak:

'Denkend aan privacy zie ik donkere wolken van vooroordelen voorbij trekken: een wat linksig en tobberig onderwerp, behandeld door actiegroepen, Registratiekamers en Datenschutzbeauftragten. Maar in de privé-sfeer ben ik altijd degene die zo vroeg mogelijk de gordijnen wenst te sluiten.'²

Toch: de behoefte aan privacy kan niet worden ontkend. Vrijwel iedereen irriteert of ergert zich aan de telefonische aanbiedingen die de avondrust of – nog erger – het favoriete televisieprogramma onderbreken. Persoonlijk ervaar ik dit als inbreuken op mijn privacy ofwel mijn persoonlijke levenssfeer. De behoefte aan privacy is altijd iets persoonlijks en dus altijd in zichzelf subjectief. Duidelijk is ook dat privacy verschillende dimensies heeft.

Deze verschillende dimensies van privacy worden in de literatuur en ook in de Grondwet onderkend. De ruimtelijke privacy: bescherming van de eigen woning (art. 12 Grondwet), de lichamelijke privacy: bescherming van de integriteit van het eigen lichaam (art. 11 Grondwet), de relationele privacy: het recht om in het maatschappelijk verkeer anoniem te blijven (het brief- en telefoongheim van art. 13 Grondwet) en tot slot de informationele privacy (art. 10 Grondwet): het recht om te bepalen welke informatie men met wie wil delen of anders gezegd: controle over hetgeen er met gegevens over jou gebeurt.

Het feit dat het begrip privacy moeilijk te definiëren is, maakt dat ook de normering ervan erg lastig is. Desondanks is privacy als een fundamenteel en universeel recht erkend.

Privacy en recht

3) In het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) uit 1950 en het Internationale Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) uit 1966 wordt het recht op bescherming van de persoonlijke levenssfeer erkend. Van groot belang voor de privacybescherming is het Verdrag van Straatsburg uit 1981 geweest. Dit verdrag beoogde de bescherming van privacy in relatie tot de geautomatiseerde gegevensregistratie te waarborgen.

4) EG Richtlijn 95/46/EG van 24 oktober 1995.

5) De vWbp volgt in grote lijnen de inhoud van de Europese privacyrichtlijn. Aanzienlijke wijzigingen worden in beginsel niet verwacht.

6) Het begrip KDD wordt veelal beperkt tot de fase van datamining. In het artikel wordt echter uitgegaan van het allesomvattende proces. Immers, een datawarehouse wordt vaak opgezet om datamining mogelijk te maken. Zie ook: M.A.J. van der Linden, *Onbekend versus onbemand, een profiel van de Wbp*, afstudeerscriptie Rechtsgeleerdheid Leiden.

7) Schreuders en Van Kralingen, *Klantenkaarten, chipcards en datamining, een juridische verkenning*, in: Van Kralingen, Lips en Prins (red.), *De kaarten op tafel, Recht, Bestuur en Informatisering*, SDU Uitgevers, Den Haag 1998.

8) Borking, Artz en Van Almelo, *Gouden bergen van gegevens*, uit de serie Achtergrondstudies en Verkenningen 10, Registratiekamer, september 1998.

Naast opname van het privacyrecht in Europese en internationale verdragen³ werd op nationaal niveau in 1983 het recht ter bescherming van de persoonlijke levenssfeer in de Grondwet opgenomen. Eenieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer, aldus artikel 10 van de Grondwet. Vervolgens wordt in hetzelfde artikel aan de overheid opgedragen regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens op te stellen. De wet dient regels te stellen inzake aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede over het recht op verbetering van zodanige gegevens.

Door de opkomst van de computer en de maatschappelijke inburgering van het gebruik van IT is steeds meer de nadruk komen te liggen op de informatiele privacy. Hierna wordt ingegaan op de wettelijke regels die de informatiele privacy beschermen en waarmee de overheid aan haar grondwettelijk opgedragen taak voldeed: namelijk de Wet persoonsregistraties. Als gevolg van de Europese privacyrichtlijn⁴ zal deze wet echter binnen afzienbare tijd moeten worden vervangen door een nieuwe wet: de Wet bescherming persoonsgegevens. Op deze laatste wet zal dan ook de nadruk worden gelegd.

Voorstel Wet bescherming persoonsgegevens

De thans geldende wet is de Wet persoonsregistraties (WPR) uit 1989. Op het moment van schrijven van dit artikel ligt het voorstel Wet bescherming persoonsgegevens (vWbp) ter behandeling bij de Tweede Kamer. Volgens de Europese privacyrichtlijn had de nieuwe wet al per eind oktober 1998 geïmplementeerd moeten zijn. Dit is helaas niet gelukt. Er is nogal commotie ontstaan over en rondom het wetsvoorstel. Zo zou het wetsvoorstel veel te gedetailleerd zijn en daardoor voor bedrijven onwerkbaar en/of te kostbare situaties creëren. VNO-NCW willen de regulering van privacy meer overlaten aan de marktpartijen (zelfregulering). De Registratiekamer is echter van mening dat een wet niet door zelfregulering (zoals door VNO-NCW en de Consumentenbond gewenst) buiten werking kan worden gesteld. Hoe het ook zij, aangenomen wordt dat het wetsvoorstel op grond van Europese regelgeving geïmplementeerd moet en zal worden. Niettegenstaande het feit dat nog geen reële inschatting kan worden gegeven van het moment waarop de vWbp in werking zal treden, doen organisaties er derhalve verstandig aan nu al rekening te houden met de vWbp⁵ voorzover deze aansluit bij de Europese privacyrichtlijn.

Overigens verschilt de structuur van de WPR niet wezenlijk met die van de vWbp. De vWbp kent evenals de WPR de volgende hoofdelementen: verplichtingen voor de gebruikers van persoonsgegevens, rechten voor degene wiens persoonsgegevens worden gebruikt en toezicht door een onafhankelijk orgaan. Toch zijn er ook verschillen. Er wordt een iets andere systematiek (die van de Europese privacyrichtlijn) gevolgd, hetgeen soms een

aanscherping, soms een versoepeling van de eisen inhoudt. Tabel 1 geeft een aantal van de belangrijkste verschillen.

In de volgende paragraaf wordt nagegaan of en zo ja, hoe de vWbp het proces van Knowledge Discovery in Databases (KDD) normeert. Teneinde dat te kunnen vaststellen is enig inzicht in het KDD-proces vereist.

Knowledge Discovery in Databases (KDD)

In dit artikel wordt onder KDD een drie fasen omvattend proces begrepen.⁶ Doelstelling van het KDD-proces is in het algemeen het voldoen aan bepaalde informatiebehoefte in een organisatie en meer in het bijzonder het afleiden van nieuwe informatie door middel van een analyse van bestaande in databases opgeslagen gegevens.⁷ De eerste fase is het opzetten van het gegevenspakhuis ofwel de datawarehouse. Dit is een database die geschikt is gemaakt voor analyse en bevraging en wordt gevuld met gegevens uit verschillende bestanden. De volgende fase is datamining. Hieronder wordt het geautomatiseerd analyseren van de in de datawarehouse opgeslagen gegevens verstaan. De laatste fase in het proces betreft het interpreteren van de analyse en het gebruik daarvan voor bepaalde doeleinden, bijvoorbeeld het gebruik van klantprofielen om gepersonaliseerde aanbiedingen te doen.

Datamining levert vijf soorten informatie op:⁸

- * *associaties*. Bijvoorbeeld: in 65 procent van de gevallen wordt er bij aankoop van een zak chips ook een fles cola gekocht.
- * *sequenties van gebeurtenissen*. Bijvoorbeeld: in 45 procent van alle gevallen zal binnen een maand na aankoop van een huis een keuken worden geplaatst.
- * *clustering van een groep mensen*. Deze vorm wordt gebruikt om binnen de geanalyseerde populatie verschillende groepen te ontdekken. Deze kennis kan weer worden benut om een bepaalde groep klanten op te sporen die belangstelling zou kunnen hebben voor een bepaald product.
- * *classificatie*. Deze vorm wordt gebruikt om typische eigenschappen van klanten of burgers te ontdekken, waarmee het gedrag van die klanten kan worden voorspeld.
- * *voorspellingen*. Hierbij gaat het om het inschatten van de toekomstige waarde van voortdurend veranderende variabelen.

De met datamining verkregen informatie is niet feitelijk. Het gaat uitsluitend om waarschijnlijkheden, die soms heel misleidend kunnen zijn. Juist dit speculatieve karakter kan leiden tot een (grotere) inbreuk op privacy.

Hierna wordt bekeken in hoeverre de voorschriften van de vWbp van toepassing zijn en wat deze betekenen voor datawarehousing en datamining als onderdeel van het KDD-proces. Daarbij wordt een toepassing van KDD, een klantkaart, als uitgangspunt genomen. Startpunt van een klantkaartproject zal zijn het bepalen van de te beantwoorden KDD-vraag: Wat is het doel van de klantkaart? De volgende stap is het inventariseren van de benodigde gegevens, het laden van de datawarehouse met de geselecteerde gegevens en al of niet aangekochte

Onderwerp	Wet persoonsregistraties	voorstel Wet bescherming persoonsgegevens
Reikwijdte (criterium voor toepasselijkheid)	<p>Aanleg of het houden van persoonsregistraties.</p> <p>Persoonsgegevens: gegevens die herleidbaar zijn tot een individuele natuurlijke persoon.</p> <p>Persoonsregistratie: een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens, die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd.</p>	<p>Iedere verwerking van persoonsgegevens.</p> <p>Persoonsgegevens: alle informatie over een geïdentificeerde of (direct of indirect) identificeerbare natuurlijke persoon.</p> <p>Verwerking: elke verzameling, vastlegging, bewaring, ordening, aanpassing, raadpleging, gebruik, verspreiding of elke andere vorm van gebruik of beschikbaarstelling van persoonsgegevens.</p>
Begrippen	<p>Houder van persoonsregistraties.</p> <p>Geregistreeerde.</p>	<p>Voor de gegevensverwerking verantwoordelijke.</p> <p>Betrokkene.</p>
Verplichtingen voor de gebruiker van persoonsgegevens		
Melding	<p>Particuliere sector: persoonsregistraties moeten worden gemeld aan de Registratiekamer.</p> <p>Overheid: opstellen van een privacyreglement.</p>	<p>Iedere gegevensverwerking of bundeling van gegevensverwerkingen dient te worden gemeld bij de Registratiekamer of bij een aangestelde privacyfunctionaris.</p>
Mededeling	<p>Mededeling van eerste opname in de persoonsregistratie aan de geregistreeerde tenzij deze 'redelijkerwijs' van de registratie 'kan weten'.</p>	<p>De mededelingsplicht wordt aangescherpt: aan de betrokkene moet voorafgaand aan de gegevensverwerking een mededeling worden gedaan tenzij deze 'op de hoogte is'.</p>
Gebruik gegevens	<p>Een persoonsregistratie wordt slechts aangelegd voor een bepaald doel waartoe het belang van de houder redelijkerwijs aanleiding geeft.</p> <p>Gegevens worden slechts gebruikt voor doeleinden die met het doel van de persoonsregistratie verenigbaar zijn.</p>	<p>Persoonsgegevens worden voor gerechtvaardigde doeleinden verzameld. Persoonsgegevens mogen slechts worden verwerkt op bepaalde in de wet aangegeven gronden, bijvoorbeeld:</p> <ul style="list-style-type: none"> * indien ondubbelzinnige toestemming van de betrokkene is verkregen; * indien de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke.
Beveiliging	<p>De houder draagt zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de persoonsregistratie.</p>	<p>De verantwoordelijke moet passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beschermen tegen een onwettige verwerking. Anders dan in de WPR wordt in de nieuwe wet uitdrukkelijk rekening gehouden met de huidige 'state of the art'-beveiligingstechnieken alsmede de kosten van tenuitvoerlegging van beveiligingsmaatregelen.</p>
Rechten van geregistreeerde personen	<p>Recht tot inzage, correctie en verwijdering van persoonsgegevens.</p>	<p>Bestaande rechten worden aangevuld met het recht van verzet: indien een gerechtvaardigd individueel belang kan worden aangetoond. In het geval van direct marketing kan altijd het recht van verzet worden ingeroepen.</p>
Toezicht	<p>De Registratiekamer houdt toezicht op naleving van de wet en is bevoegd een onderzoek uit te voeren.</p>	<p>Bevoegdheden van de Registratiekamer worden uitgebreid. De Registratiekamer kan nu ook bestuursdwang toepassen.</p>

Tabel 1.
Vergelijkend overzicht
WPR en vWbp.

gegevens (datawarehousing), waarna de analyse van de gegevens (datamining) wordt uitgevoerd. De laatste stap is het gebruik van de klantprofielen om bijvoorbeeld

gepersonaliseerde aanbiedingen te doen. Een individuele klant wordt in een bepaald klantprofiel ingedeeld en dienovereenkomstig behandeld (classificatie).

KDD, klantkaarten en het voorstel Wet bescherming persoonsgegevens

Of de vWbp van toepassing is, hangt allereerst van de reikwijdte af. De vWbp is van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens alsmede op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Daarvan zal in het KDD-proces wel snel sprake zijn. Onder persoonsgegevens wordt vervolgens alle informatie verstaan betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. In de meeste gevallen heeft de klant in ruil voor de klantkaart op een formulier naam, adres, leeftijd en wellicht andere gegevens ingevuld. De gegevens op een dergelijk formulier zijn zonder meer persoonsgegevens. Deze zijn, mits de betrokken persoon zijn adresgegevens juist invult, direct te identificeren. Het met het KDD-proces verkregen klantenprofiel is echter op zichzelf geen persoonsgegeven, het gaat immers om een groep van personen die in een profiel passen. Echter, door de koppeling van het formulier en de betreffende klantkaart is inkoopgedrag herleidbaar tot een individuele klant. Bij het ontdekken van de (nieuwe) kennis gaat het op enig moment in de fase van het KDD-proces dus toch om persoonsgegevens.

Zoals gezegd is de vWbp van toepassing op iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Gesteld kan worden dat het KDD-proces en daarmee het gebruik van klantkaarten onder het bereik van de vWbp valt. Overigens stelt de Memorie van Toelichting⁹ bij het wetsvoorstel uitdrukkelijk dat de gegevensverwerking voor datamining onder de normering van de vWbp valt.

Wat betekent dit nu voor een onderneming die een klantkaart uitgeeft en daarmee informatie over klanten vergaart? Welke verplichtingen legt de vWbp in dit verband op?

In alle fasen van een klantkaartproject moeten de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt. Gedoeld wordt op het principe van doelbinding, rechtmatigheid van de gegevensverwerking (c.q. de gronden waarop gegevens mogen worden verwerkt) en de waarborging van rechten van betrokkenen (geregistreerden).

Persoonsgegevens mogen worden verwerkt indien ondubbelzinnige toestemming is verkregen.

Doelbinding

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Dit betekent dat een onderneming geen gegevens mag verzamelen zonder een precieze doelsomschrijving. Dit sluit aan bij het KDD-proces. Dit proces kan niet van start gaan zonder een bepaalde vraag-

stelling op grond waarvan de benodigde gegevens worden geïnventariseerd, geselecteerd en geanalyseerd.

Voordat een onderneming rechtmatig met het verzamelen van klant- en aankoopgegevens begint, moet de onderneming het doel hebben omschreven en daarvan ook mededeling hebben gedaan aan de betrokkene. Veelal geschiedt dit laatste door middel van het aanmeldingsformulier.

Voorts mogen de gegevens alleen voor gerechtvaardigde doeleinden worden verzameld. Een doeleinde is gerechtvaardigd indien de gegevens worden verwerkt voor één van de gronden als genoemd in de vWbp.

Rechtmatige gegevensverwerking

Persoonsgegevens mogen slechts worden verwerkt indien:

- a de betrokkene (van wie gegevens worden verwerkt) daarvoor ondubbelzinnige toestemming heeft verleend, of
- b de verwerking noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene partij is, of
- c de verwerking noodzakelijk is om een wettelijke plicht waaraan de verantwoordelijke is onderworpen na te komen, of
- d de gegevensverwerking noodzakelijk is ter bestrijding van ernstig gevaar voor de gezondheid van de betrokkene, of
- e de gegevensverwerking noodzakelijk is voor de vervulling van een publieke taak door een bestuursorgaan, of
- f de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de gegevensverwerking verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang van de betrokkene (het recht op privacy) prevaleert.

De gronden genoemd onder c en e zijn in het kader van een klantkaart evident niet van belang. De gegevensverwerkingen die voortvloeien of samenhangen met een klantkaart zijn ook niet noodzakelijk voor de uitvoering van een overeenkomst (b) of noodzakelijk ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene (d).

Persoonsgegevens van klanten mogen verwerkt worden indien dit geschiedt met ondubbelzinnige toestemming van de betrokkene. Toestemming wordt gedefinieerd als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. Is het invullen van een aanmeldingsformulier als 'ondubbelzinnige' toestemming op te vatten? Het ondertekenen van een formuleer dat een algemene machtiging tot gegevensverwerking inhoudt, is geen specifieke wilsuiting.¹⁰ Kortom, het aanmeldingsformulier moet dusdanige informatie bevatten dat het voor de betrokkene zonder meer duidelijk is dat zijn gegevens worden verwerkt en voor welke doeleinden. Opgemerkt wordt dat bij twijfel over het al dan niet verleend hebben van een ondubbelzinnige toestemming, de bewijslast op de verantwoordelijke rust. De betreffende onderneming moet aantonen

9) TK 1997-1998, 25 892, nr. 3, p. 52.

10) TK 1997-1998, 25 892, nr. 3, p. 65.

dat de toestemming aan de gestelde eisen voldoet. Daarnaast moet worden aangetoond dat de onderneming op het punt van informatieverstrekking alles heeft gedaan wat redelijkerwijs van haar mocht worden verwacht.¹¹

Eventueel zou de onderneming de gegevensverwerking in het kader van een klantkaart kunnen scharen onder grond f. Onderdeel f is algemener van aard en daarmee een soort restbepaling, aldus de Memorie van Toelichting bij de vWbp. In beginsel is het werven en het binden van klanten een gerechtvaardigd commercieel belang. Hierbij spelen echter het zogenaamde subsidiariteits- en het proportionaliteitsbeginsel een rol.¹² Kan het doel dat met de verwerking wordt nagestreefd ook langs een andere weg (zonder verwerking) worden bereikt en is de verwerking evenredig aan het nagestreefde doel? De verantwoordelijke moet zich dus de vraag stellen of de voorgenomen gegevensverwerking, alle belangen (privacy) in aanmerking genomen, noodzakelijk is voor het doeleinde van de gegevensverwerking. Die vraag voert te ver om in dit artikel te beantwoorden. Hier spelen ook bedrijfseconomische aspecten een rol. Zekerheidshalve zou een onderneming beter kunnen uitgaan van een ondubbelzinnige toestemming van de betrokkene. Los daarvan is de voor de gegevensverwerking verantwoordelijke verplicht informatie over de gegevensverwerking te verstrekken aan de betrokkene.

Overigens gelden voor zogenaamde 'gevoelige gegevens' speciale regels. Dit zijn gegevens over politieke gezindheid, levensovertuiging, godsdienst, ras, seksuele leven en lidmaatschap van vakverenigingen. Deze mogen op grond van de vWbp in beginsel niet worden verwerkt tenzij betrokkenen hiervoor nadrukkelijk toestemming hebben verleend of de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang dan wel indien de wet dat uitdrukkelijk toestaat.

Rechten van betrokkenen (geregistreerden)

Indien de betrokkene zelf gegevens ter beschikking stelt, is de verantwoordelijke verplicht vóór het moment van de verkrijging van gegevens, informatie te verstrekken over zijn identiteit en de doeleinden van de verwerking (tenzij de betrokkene daarvan reeds op de hoogte is). Bovendien zal de verantwoordelijke nadere informatie moeten verstrekken, onder meer gelet op de aard van de gegevens en het gebruik ervan, als dat nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. In het geval van een klantkaart is het aannemelijk dat deze nadere informatie moet worden verstrekt. Het is voor de klant immers niet bij voorbaat duidelijk dat met de klantpas niet alleen kortingen kunnen worden verkregen, maar dat met behulp van de klantpas gegevens worden verkregen die geanalyseerd worden.

Ten aanzien van verwerkingen die verband houden met direct marketing is aan de betrokkene een recht van verzet toegekend. Onder direct marketing verstaat de Memorie van Toelichting:¹³ het systeem gericht op het tot stand brengen of in stand houden van een directe relatie tussen aanbieder en diens afnemers. Het uitgeven van een klantkaart is als zodanig te beschouwen. Dit betekent dat een betrokkene c.q. de houder van de klant-

kaart te allen tijde verzet kan aantekenen. De betreffende onderneming dient de gegevensverwerkingen dan terstond te beëindigen. Naast bovenstaande rechten heeft de betrokkene het recht, indien gegevens feitelijk onjuist, onvolledig of niet ter zake doende zijn, de gegevens te laten verbeteren, aanvullen, verwijderen of afschermen.

Conclusie

In het voorgaande is vastgesteld dat het wetsvoorstel Wet bescherming persoonsgegevens op het KDD-proces van toepassing is. Transparantie, rechtmatige gegevensverwerking, doelbinding, rechten van betrokkenen en beveiliging zijn de kernbegrippen uit deze wet. Anders gezegd: personen moeten weten welke gegevens over hen worden verzameld en moeten enige zeggenschap hebben over wat er met deze gegevens gebeurt. De door de wet gestelde algemene normen voor een zorgvuldige gegevensverwerking bieden in beginsel voldoende ruimte om het privacybelang van de betrokkene te kunnen beschermen en lijken, in tegenstelling tot andere berichten in de media,¹⁴ geen barrière te vormen voor toepassing van KDD (en het gebruik van klantkaarten als middel tot klantenbinding). Met inachtneming van de wet kan een onderneming ervan uitgaan dat zij zorgvuldig omgaat met de klantgegevens en dus met de klant. Indien de onderneming voldoende open is over het gebruik van de gegevens en zorgvuldig ermee omgaat, zal een klant eerder bereid zijn (de juiste) gegevens te verstrekken. Dit komt het KDD-proces alleen maar ten goede. In ieder geval zou de klant het laatste woord moeten hebben over hetgeen er met zijn gegevens gebeurt. De klant is immers koning.

11) TK 1997-1998, 25 892, nr. 3, p. 68.

12) TK 1997-1998, 25 892, nr. 3, p. 79.

13) TK 1997-1998, 25 892, nr. 3, p. 170.

14) Anders dan bepaalde publicaties suggereerden, zie bijvoorbeeld Automatisering Gids 1998, nr. 15, p. 21: *Nieuwe wet legt analyse klantgegevens aan banden.*