

# De gevolgen van het *Dexia*-arrest voor de praktijk

310

## Trefwoorden:

inzagerecht, informatiebehoefte, ontsluiting van informatie, customer data beheer, verwijfsindex, datawarehousing

Dit artikel schetst de operationele gevolgen van het inzagerecht voor instellingen naar aanleiding van het *Dexia*-arrest. Leidt dat arrest bijvoorbeeld tot een meer gedetailleerde melding bij het CBP en uitgebreidere informatie aan betrokkene?

Een organisatie dient in vier weken te voldoen aan het verzoek om inzage. Dit artikel laat zien dat in de praktijk veel problemen overwonnen moeten worden om een inzageverzoek snel en correct te kunnen afhandelen. Het inrichten van customer data beheer en het gebruik van verwijfsindexen en datawarehousing bieden daarbij uitkomst, waarbij het accent dient te liggen op het helder krijgen van de informatievraag en het ontwikkelen van een standaard query.<sup>2</sup>

## 1 Aanleiding

In juni 2007 heeft de Hoge Raad een drietal arresten<sup>3</sup> gewezen over de reikwijdte van het inzagerecht van art. 35 Wet bescherming persoonsgegevens (WBP). In alle drie de zaken vragen de klanten van hun bank een volledig overzicht van persoonsgegevens die de bank heeft verwerkt. Daarbij vragen de klanten in het bijzonder om kopieën van documenten waarop hun persoonsgegevens voorkomen, zoals formulieren, cliëntprofielen, contracten, aankoopbewijzen en transcripties van telefoongesprekken. De klanten beroepen zich met hun verzoek op art. 35 WBP, dat betrokkenen een inzagerecht geeft in hun persoonsgegevens die instellingen over hen bijhouden.

Art. 35 WBP verplicht de banken om de klanten binnen vier weken na ontvangst van het verzoek schriftelijk mee te delen of hen betreffende persoonsgegevens worden verwerkt. Zo ja, dan dient er een volledig overzicht daarvan in begrijpelijke vorm te worden gegeven, waarbij ook informatie dient te worden verstrekt over het doel van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.

De banken hebben daartegen bezwaren aangevoerd. Zo

vreesde een bank grote administratieve lasten als duizenden procederende klanten het voorbeeld van de twee verzokende klanten zouden gaan volgen. De andere bank vond zijn recht op een eerlijk proces geschonden als het zelf munitie aan de procederende klant zou moeten verschaffen. Beide banken vonden dat ook aan het inzagerecht werd voldaan als aan de klant een begrijpelijke samenvatting van het klantdossier werd gegeven.

## 2 Strekking arresten

De Hoge Raad oordeelt dat aan het wettelijk recht op inzage een ruime uitleg moet worden gegeven. Dat betekent dat geen samenvatting maar alle relevante informatie over betrokkene moet worden verschaft, hetgeen vaak zal kunnen gebeuren door het verstrekken van afschriften, kopieën of uittreksels. Ook notities die bij derden zijn opgevraagd vallen onder het inzagerecht; alleen interne notities die de persoonlijke gedachten van medewerkers bevatten niet, omdat het daar minder vanzelfsprekend voor is dat deze bedoeld zijn om tezamen met andere persoonsgegevens in een bestand te worden opgenomen.

Kortom, er dient een overzicht van concrete gegevens te worden verstrekt die van een betrokkene zijn vastgelegd in een papieren dossier en in een elektronische administratie. Voorts moeten ook kopieën van bescheiden, microfilm en transcripties van telefoongesprekken worden gegeven, voor zover aanwezig en de betrokkene daarom verzoekt. Het doel van het inzagerecht is om te kunnen nagaan of, en zo ja, welke gegevens er worden verwerkt, en of die gegevens juist en volledig zijn en in verband met het doel ter zake dienend. Anders gezegd: de betrokkene kan door het uitoefenen van zijn inzagerecht de rechtmatigheid en de juistheid van de gegevensverwerking van zijn persoonsgegevens nagaan. Indien de gegevens feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel van verwerking, dan kan de betrokkene de instelling verzoeken om de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Daarnaast overwoog de Hoge Raad dat voor een op art. 35 WBP gebaseerd verzoek geen bijzondere redenen behoeven te worden opgegeven.

Voorts geeft de Hoge Raad aan dat van het recht uiteraard geen misbruik mag worden gemaakt en dat de uitoefening ervan evenmin mag leiden tot een disproportionele belasting van de verantwoordelijke bank of tot aantasting van de rechten of belangen van derden.

en bijvoorbeeld ook de prijzen van de woonhuizen en telefoonnummers bevat kan de query uitgebreid worden met de vraag: Maak een lijst met namen en telefoonnummers van mensen die wonen in een huis dat tussen de 100 000 en 200 000 euro heeft gekost.

1 Ellen Hoving is directeur van Compliance & Advisory, een adviesbureau op het gebied van Compliance en privacy ([www.Compliance-Advisory.com](http://www.Compliance-Advisory.com)).

2 Met een query (vraagstelling) wordt in de informatica een opdracht bedoeld die aan een database wordt gegeven om een bepaalde actie uit te voeren, die ook potentieel gegevens teruggeeft. Een voorbeeld van een query uit een database met namen en adressen kan zijn: maak een lijst van alle personen uit de database die in Amsterdam wonen. Als de database uitgebreider is

3 Zie de zaken *Dexia/verweerder S* (zaaknr. R06/045, LJN AZ4663) en *Dexia/verweerder* (zaaknr. R06/046, LJN AZ4664) en *HBU tegen G. c.s.* (zaaknr. R06/163, LJN BA3529) en het artikel van prof. dr. P.J.A. de Hert e.a. 'De WBP na de *Dexia*-uitspraken', *P&I* 2007, p. 147 e.v.

Het kostenaspect, gelet op de vele inzageverzoeken, levert geen weigeringsgrond op in de zin van art. 43, onderdeel e WBP. Dit is een risico dat verbonden is aan het hebben van een groot klantenbestand. Bovendien kan voor het doen van een inzage van de betrokkene een (gemaximeerde) bijdrage in de kosten worden verlangd.

### 3 Consequenties voor de praktijk

Welke consequenties heeft dit uitgebreide inzage-recht voor de praktijk? De juridische consequenties van de arresten zijn al besproken in het in noot 3 genoemde artikel van De Hert en anderen, en komen derhalve niet meer aan de orde.

Aan de orde komt wat het uitgebreide inzage-recht betekent voor de bedrijfsvoering van de instelling. In feite vraagt het van een organisatie dat zij de informatievoorziening met betrekking tot persoonsgegevens structureel heeft belegd. Zij dient daarbij een helder beeld te hebben ten aanzien van de volgende punten:

- In het kader van welke doeleinden worden persoonsgegevens verwerkt binnen de organisatie?
- Van wie worden persoonsgegevens ontvangen (inkoop van data) en aan wie worden data verstrekt (de ontvangers)?
- Waar bevinden die persoonsgegevens zich in de organisatie?
- En wie kan daarvoor worden aangesproken?

De organisatie moet immers in vier weken kunnen voldoen aan het verzoek om inzage. Dit artikel laat zien, dat het stellen van die vragen gemakkelijker is dan ze te beantwoorden en dat in de praktijk veel voetangels en klemmen overwonnen moeten worden om een inzageverzoek snel en correct te kunnen afhandelen.

### 4 Gevolgen van de arresten met betrekking tot de melding en de informatieplicht

#### 4.1 Melding aan het CBP

Volgens art. 27 en 28 WBP is een instelling die persoonsgegevens verwerkt verplicht tot een melding van de gegevensverwerking bij het College bescherming persoonsgegevens (CBP).

In de melding is opgenomen welke gegevens worden verwerkt voor welke doeleinden.

Indien andere gegevens worden verzameld dan gemeld aan het CBP, dan zal de melding moeten worden aangepast.

#### 4.2 De informatieplicht

De betrokkene, bijvoorbeeld een klant, moet kunnen weten wie welke persoonsgegevens over hem verzamelt en op welke wijze deze gegevens worden verwerkt. De verantwoordelijke is dus verplicht de betrokkene te informeren. Art. 33 en 34 WBP bevat de regeling hoe de informatieverstrekking aan de betrokkene dient plaats te vinden. De organisatie moet betrokkenen informeren over het doel van de gegevensverwerking en de identiteit van de verantwoordelijke. In sommige gevallen moet aan de betrokkene meer informatie

over het gebruik van zijn persoonsgegevens gegeven worden. Denk daarbij aan:

- de verwachtingen van de betrokkene indien het gebruik anders is dan de betrokkene redelijkerwijs kan verwachten;
- de omstandigheden waaronder de organisatie de gegevens krijgt;
- het gebruik dat de organisatie ervan gaat maken;
- de aard van de gegevens. Hoe gevoeliger de aard van de gegevens die de organisatie van betrokkene gebruikt, hoe meer reden er is om betrokkene hierover gedetailleerd te informeren.

De vraag is nu of het uitgebreide inzage-recht leidt tot een meer gedetailleerde melding bij het CBP en informatievoorziening aan de betrokkenen. Het inzage-recht geeft – zoals de Hoge Raad nu ook heeft bevestigd – de betrokkene recht op gedetailleerde informatie over welke gegevens er worden verwerkt, met welk doel, de categorie van gegevens, de ontvangers en herkomst van gegevens en betrokkene krijgt daarbij de beschikking over allerlei documenten en mogelijk tapes of andere informatiedragers. Sommige van deze gegevens dienen opgenomen te zijn in de melding aan het CBP ofwel te worden meegegeeld aan betrokkene via de informatieverplichting. Uit de praktijk blijkt dat de meldingen nogal ruime doelomschrijvingen bevatten en dat de informatieteksten die instanties verstrekken op hun documenten of anderszins heel globaal zijn geformuleerd.

#### 4.3 Match gegevens uit de diverse plichten

Belangrijk voor betrokkene is dat er een match ontstaat tussen de gegevens bekend uit de meldingen aan het CBP, de gegevens die hijzelf in het kader van de informatieplicht heeft ontvangen en de gegevens die hij ontvangt in het kader van het uitgeoefende inzage-recht. Dat betreffen veelal gegevens in het kader van de verdere verwerking in de bedrijfsvoering van de verantwoordelijken en anderen, zoals de ontvangers. Indien de betrokkene de informatie niet kan plaatsen, roept dat al snel vraagtekens op met betrekking tot verenigbaar gebruik. Verenigbaar gebruik wil zeggen dat er een verwantschap moet zijn tussen het doel van een verdere verwerking van een persoonsgegeven en het doel waarvoor de gegevens zijn verkregen. Zo kan bijvoorbeeld de informatie verzameld in het kader van het sluiten van een levensverzekering, niet zo maar worden gebruikt in het kader van het sluiten van een kredietovereenkomst.

Gegevens die een betrokkene mogelijk niet zo maar kan plaatsen zijn bijvoorbeeld zijn creditscore, zijn klantprofiel, informatie over zijn internetgedrag, hoelang hij een site bezoekt en welke pagina's, en data verkregen van derden in het kader van bijvoorbeeld marketingacties. Vragen die dan rijzen zijn: in het kader van welk doel zijn welke gegevens verzameld en is betrokkene daarover geïnformeerd? Is de verwerking rechtmatig en noodzakelijk?

Hoe concreter de betrokkene al is geïnformeerd via de melding en de informatieplicht des te kleiner is de kans op een mismatch en schijnbaar onverenigbaar gebruik, omdat

het doel, het kader van de verdere verwerking en de soort van gegevens al bekend zijn bij betrokkene.

In de praktijk kan de schoen gaan wringen, omdat er een mismatch kan ontstaan tussen de globale gegevens bekend aan de klant via de melding aan het CBP en de informatieplicht en de gedetailleerde gegevens die hem nu moeten worden meegedeeld in het kader van zijn inzage-recht. Om dat te voorkomen zullen instellingen mogelijk in de melding en informatievoorziening wat concreter de doeleinden van verwerking moeten omschrijven en aangeven welke gegevens zij daarbij verwerken.

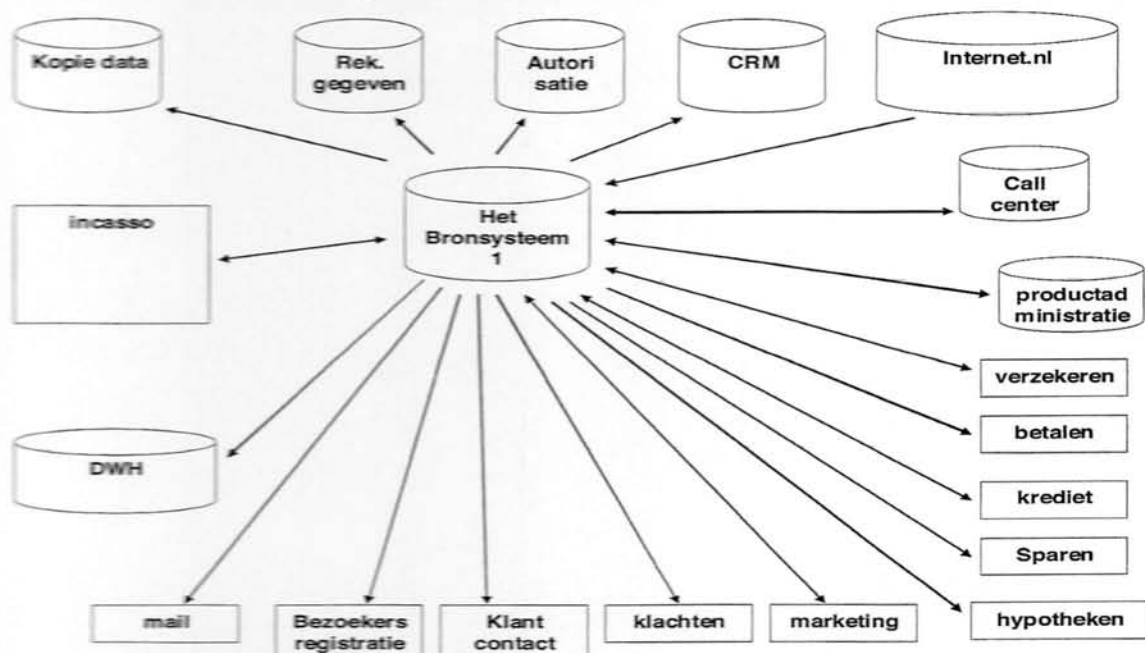
## 5 Consequenties van de arresten voor de bedrijfsvoering

### 5.1 Informatiebehoefte en ontsluiting van gegevens

Aan de verzoeken om inzage valt op zich prima te voldoen als dat maar een paar verzoeken per jaar zijn of als het gegevens betreffen gerelateerd aan één financiële dienst. Het wordt al lastiger aan een verzoek om inzage te voldoen als het aantal verzoeken flink toeneemt, zoals bij een bank uit de casus, die ruim 3900 verzoeken had binnen gekregen of zoals het geval is bij het BKR, waar in 2006 117 000 inzageverzoeken zijn ingediend.<sup>4</sup> Een andere factor die het honoreren van een inzageverzoek lastig maakt, is als een klant verschillende soorten van financiële diensten afneemt bij verschillende onderdelen van een omvangrijk financieel conglomeraat en daarbij gebruik maakt van verschillende media zoals internet, mail en call centers.

Het volgende plaatje illustreert deze problematiek:

### Schematische weergave klantdata



### 5.2 Schets gegevensverwerking in de praktijk

Zoals bovenstaand plaatje illustreert hebben organisaties vaak zeer veel gegevens vastgelegd in honderden systemen die vele operationele processen ondersteunen. In een organisatie worden persoonsgegevens ingevoerd, gemuteerd en geraadpleegd in processen binnen de front-office, mid- en backoffice, ondersteund door informatiesystemen.

Om data te kunnen ontsluiten en een correct gebruik daarvan te kunnen waarborgen moet het verband helder zijn tussen enerzijds de persoonsgegevens in de diverse informatiesystemen en anderzijds de organisatieprocessen en verantwoordelijkheden waarbinnen deze persoonsgegevens worden ingevoerd, gemuteerd, geraadpleegd en uitgeleverd.

Veelal ontbreekt bovengenoemd verband door de volgende oorzaken:

1. Er zijn veel systemen en databases binnen een organisatie, maar een sluitende administratie van alle systemen ontbreekt soms. Er zijn deeladministraties, bijvoorbeeld gericht op een afdeling. Er zijn administraties die door alle afdelingen worden gebruikt die niet volledig zijn ingevuld en/of niet de voor de afdeling relevante gegevens bevatten.
2. De systemen worden technisch, operationeel en functioneel beheerd. Maar wie verantwoordelijk is voor de data in deze systemen is niet altijd bekend. Dit geldt temeer indien applicaties of databases door meerdere kanalen of labels worden gebruikt. Wie is bijvoorbeeld aanspreekbaar op de juistheid en volledigheid van de persoonsgegevens? Er is niet altijd de garantie dat persoonsgegevens actueel of up-to-date zijn. Daarnaast wordt de aanwezigheid van klantdata in systemen vaak ook niet geregistreerd.

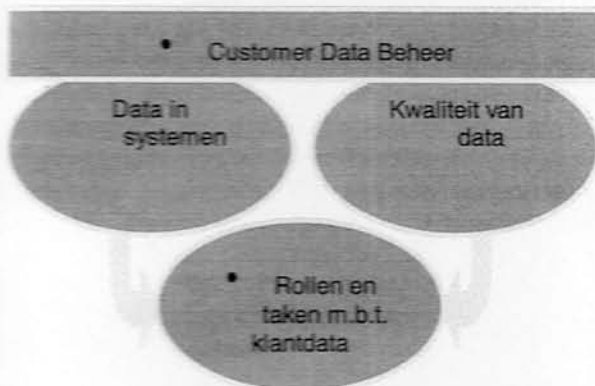
<sup>4</sup> BKR jaarverslag 2006 en P&I 2007, p. 175-176.

5.3 *Informatiebehoefte in verband met het inzagerecht*  
Gelet op de hierboven geschetste gegevensverwerking in de praktijk wordt het lastig in het kader van een inzageverzoek de volgende vragen beantwoord te krijgen:

1. Welke klantgegevens heeft de organisatie nodig om aan het verzoek te kunnen voldoen?
2. Waar zitten die klantgegevens?
3. Van wie zijn de data verkregen en aan wie zijn ze verstrekt?
4. In welke vorm zijn die klantgegevens vastgelegd, is dat
  - papier?
  - e-mail, internet, sms of msn?
  - microfilm of -fiche?
  - image opgeslagen op cd-rom/dvd?
  - data opgeslagen op tapes?
  - data opgeslagen in databases, servers e.d.?

Wie kan aangesproken worden om die klantgegevens boven water te krijgen?

Om als organisatie deze vragen structureel beantwoord te krijgen, vereist dat een verantwoordelijkheidsstructuur, waarin wordt bepaald wie verantwoordelijk is voor de (klant) data en de kwaliteit van die data. Dit geschiedt veelal door het opzetten van customer data beheer.



Indien een instelling customer data beheer heeft opgezet, dan zijn de volgende onderdelen met betrekking tot de informatievoorziening structureel belegd in de organisatie en is het ook bekend wie daarvoor verantwoordelijk is:

1. Er is een bedrijfsmodel persoonsgegevens wat inhoudt dat de organisatie en de onderliggende informatievoorziening in kaart is gebracht. Het is bekend op welke plaatsen persoonsgegevens worden gecreëerd, gemonteerd, geraadpleegd en uitgeleverd. Er is overzicht van de belangrijkste relatie- en productiesystemen per bedrijfs-onderdeel.
2. Binnen elk bedrijfs-onderdeel liggen de rollen, taken en verantwoordelijkheden rondom de persoonsgegevens vast, bijvoorbeeld in de zin van:

- De leverancier is verantwoordelijk voor de initiële kwaliteit van het gegeven.
  - De verantwoordelijke is verantwoordelijk voor het juiste gebruik van het gegeven.
  - De beheerder is verantwoordelijk voor het bewaren van het gegeven en het in stand houden van de kwaliteit (juistheid, consistentie).
  - De verwerker mag het gegeven gebruiken binnen de (door de verantwoordelijke of beheerder) gestelde kaders.
3. De persoonsgegevens en de organisatie rondom persoonsgegevens worden centraal vastgelegd in een register, dat wordt bijgehouden.

#### 5.4 *Chief information officer customer domain*

Om het proces van customer data beheer te vergemakkelijken is het wenselijk een specifieke functie in het leven te roepen, zoals een chief information officer of een afdeling customer domain. Deze is verantwoordelijk voor het adequaat beleggen en functioneren van customer data beheer in de organisatie en daarnaast kan deze belast worden met de volgende taken:

- het vaststellen van het beleid en de normen voor customer data en het bewaken van de kwaliteit daarvan;
- het vaststellen van eisen met betrekking tot gebruik en beheer van data in klantprocessen, in de back-office en bij externe partijen;
- de regie met betrekking tot het sluiten van overeenkomsten met bewerkers van persoonsgegevens, de data inkoop en het bijhouden van een contractenregister;
- het stellen van eisen met betrekking tot interne en externe klantdata voor marketing doeleinden en analyse, en
- een sluitende registratie van de systemen waarin persoonsgegevens worden verwerkt en van welke data zich daarin bevinden.

Met het inrichten van customer data beheer wordt duidelijk wie in een organisatie verantwoordelijk is voor persoonsgegevens. Daarmee is nog niet direct het probleem opgelost welke data ontsloten dienen te worden naar aanleiding van een inzageverzoek. Immers, welke data zijn er nodig om aan een inzageverzoek te voldoen en hoe krijg je die data tot je beschikking?

#### 5.5 *Technieken om de juiste gegevens te ontsluiten en te verzamelen*

In de loop der tijd zijn specifieke technologieën ontstaan om gegevens te verzamelen en te analyseren, zoals het koppelen van bestanden en *knowledge discovery in databases* (datamining).<sup>5</sup> Deze technieken zijn ook bruikbaar voor het ontsluiten van informatie in verband met het inzagerecht. Met betrekking tot het inzagerecht zijn twee onderdelen bruikbaar, te weten verwijzindexen en datawarehousing. Het accent ligt daarbij op het helder krijgen van de informatie-vraag. Het gaat daarbij uiteraard om klantgegevens die zijn

bergen van gegevens', zie Achtergrondstudies en Verkenningen nr. 10 van de Registratiekamer.

5 Meer informatie over deze problematiek is te vinden in het proefschrift van Eric Schreuders, *Datamining, de toetsing van beslisseregels & privacy*, <[www.privacydossier.nl](http://www.privacydossier.nl)> en in 'Gouden

opgeslagen in elektronische bestanden en dus niet de klantgegevens die zijn vastgelegd op papier.

Een verwijfsindex is, kort gezegd, een bestand waarin staat in welke bestanden ook (en vooral) gegevens over een bepaalde persoon zijn opgenomen. De gegevens zelf uit de verschillende bestanden worden daarbij niet of zeer beperkt in de verwijfsindex opgenomen. Met verwijfsindexen kan afzonderlijk informatiebeheer worden 'overkoepeld' met centrale bestanden, waardoor de gegevens in de verschillende bestanden waar naar verwezen wordt als het ware toch bijeen gebracht worden. De facto blijven de gegevens in de verschillende bron- en productsystemen staan, echter door de verwijfsindex is wel bekend in welke bestanden welke gegevens zijn opgenomen.

Gegevens binnen een organisatie zijn opgeslagen in vele verschillende operationele bestanden. Bij datawarehousing worden de verspreide gegevens uit de verscheidene bron- en productsystemen verzameld en opgeslagen in een database, genaamd het datawarehouse. In het datawarehouse worden de gegevens toegankelijk gemaakt voor nader onderzoek en analyse, teneinde aan een bepaald informatieverzoek te voldoen. Datawarehousing bestaat kort gezegd uit het verzamelen, verrijken, schonen en coderen van gegevens.

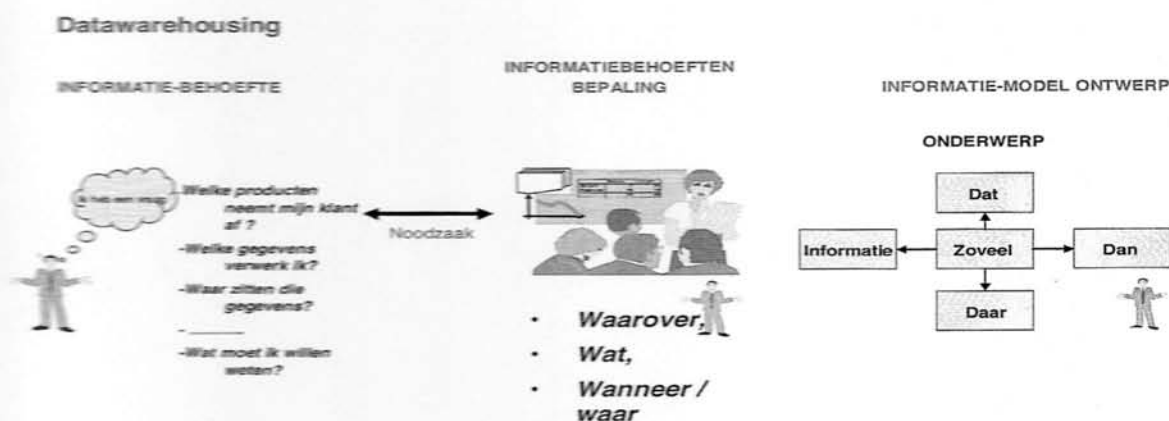
Het belangrijkste doel van het datawarehouse is om de gegevens op zodanige wijze op te slaan dat er op een eenvoudige en snelle manier informatie uit gehaald kan worden, die voorziet in een specifieke informatiebehoefte. In casu dus de persoonsgegevens om aan het inzageverzoek te voldoen.

Voordat gestart wordt met het analyseren van data wordt een bestand aangelegd dat ingericht is op het verrichten van de analyses. Dit bestand is het datawarehouse. Vervolgens vindt controle op de juistheid van de gegevens plaats.

Schreuders<sup>6</sup> onderscheidt daarbij twee elementen: formele en materiële juistheid. Bij formele juistheid moet vooral worden gedacht aan de afwezigheid van invoerfouten en aan de integriteit van de data (is het ingevoerde adres een bestaand adres). Bij materiële juistheid gaat het om de relatie tussen de gegevens en de juistheid: is het juist getypte en ook bestaande adres ook het échte adres van de betrokken persoon. Controle op juistheid is een belangrijk aspect voor de kwaliteit van de uit het datawarehouse aangeleverde informatie.

De technologie van verwijfsindexen en datawarehousing faciliteert het verkrijgen van informatie naar aanleiding van een inzageverzoek. Die technieken zijn te gebruiken om vast te stellen welke informatie je nodig hebt, waar die informatie zich bevindt, waar die informatie verzameld wordt en welke informatie uiteindelijk aan betrokkene kan worden meegegeeld.

Belangrijk in deze systematiek is dat het accent ligt op het helder krijgen van de informatievraag en niet zozeer de techniek, zoals het bouwen van het datawarehouse. De structuur binnen het datawarehouse of de verwijfsindex wordt in eerste instantie bepaald door de informatievraag: het doel is te bepalen welke gegevens er nodig zijn, waar die zijn opgeslagen, hoe ze ontsloten worden en wat daarover wordt gerapporteerd. Het is verstandig om een standaard query te ontwikkelen en een verwijfsindex samen te stellen, zodat in feite maar één keer het informatiemodel doorlopen hoeft te worden. Dan heeft de organisatie een standaardproces om na te gaan welk soort van persoonsgegevens er nodig is en waar deze gegevens zijn opgeslagen. Schematisch ziet het informatievoorzieningsproces er als volgt uit:



<sup>6</sup> Zie par. 3.3.2.1.1 op p. 30 in voormeld proefschrift van Eric Schreuders, *Datamining, de toetsing van beslisregels & privacy*.

Indien het daarbij gewenst is om de bron- en productsystemen zo min mogelijk te belasten met de uitvraag van gegevens, dan is het aan te bevelen om regelmatig kopieën van primaire processystemen te maken en die in een apart bestand te zetten. Belangrijk is ook aandacht te besteden aan de formele en materiële juistheid van de data, zodat de betrokkene correcte data ontvangt.

Het voordeel van het gebruik van bovenstaande technieken is dat er een standaardmethodiek wordt ontwikkeld, die op een adequate wijze de benodigde informatie kan verschaffen bij een inzageverzoek. Dit geldt overigens niet alleen voor elektronische bestanden, maar ook voor informatie opgeslagen op andere informatiedragers zoals papier. Het biedt de mogelijkheid tot correcte en volledige uitvraag van de gewenste informatie en dit leidt tot een zorgvuldige beantwoording van het inzageverzoek van de klant. Deze manier van werken verdient verreweg de voorkeur in plaats van de nu veelal ad-hocbeantwoording van een verzoek om inzage, welk verzoek nogal eens leidt tot een willekeurig in productsystemen opzoeken van data van de betrokkene. Een tweede voordeel van de systematische aanpak is dat de opgevraagde informatie kan worden afgestemd op de informatiebehoefte. En er wordt geen overbodige informatie opgevraagd en ingezien.

Tot slot een organisatorisch punt: om de ingekomen inzageverzoeken ook administratief adequaat af te kunnen handelen en overzicht te krijgen over de hoeveelheid aanvragen, dient de organisatie een centraal punt in te richten waar de inzageverzoeken binnenkomen, worden geregistreerd, in behandeling worden genomen en worden afgewikkeld.

## 6 Conclusie

De Hoge Raad oordeelt dat aan het wettelijk recht op inzage een ruime uitleg moet worden gegeven. In de praktijk kan de schoen gaan wringen indien er een mismatch ontstaat tussen enerzijds de globale gegevens zoals die via de melding aan het CBP en de uitvoering van de informatieplicht bij de klant bekend zijn, en anderzijds de gedetailleerde gegevens die hem nu moeten worden meegedeeld in het kader van zijn inzagerecht. Om deze mismatch te voorkomen zullen instellingen mogelijk in de melding en in de meegedeelde informatie op grond van de informatieverplichting concreter de doeleinden van verwerking moeten omschrijven en concreter aan moeten geven welke gegevens zij daarbij verwerken.

Aan de verzoeken om inzage valt op zich prima te voldoen als dat er maar een paar per jaar zijn. Het wordt lastiger daaraan te voldoen als het aantal flink toeneemt en als een betrokkene verschillende soorten diensten afneemt bij verschillende onderdelen van een instelling. Nog lastiger wordt dit als de betrokkene gebruik maakt van verschillende media zoals internet, mail en call center.

Gezien het feit dat binnen een organisatie de verantwoordelijkheden voor het gebruik van persoonsgegevens veelal niet belegd zijn en de operationele processen niet zijn ingericht voor het ontsluiten van persoonsgegevens naar aanleiding van het inzagerecht, wordt de vraag pregnant op

welke wijze dat wel zou kunnen geschieden. Met het inrichten van customer data beheer wordt er een verantwoordelijkheidsstructuur gecreëerd met betrekking tot klantdata en kwaliteit. Daarmee is overigens nog niet direct het probleem opgelost welke data ontsloten dienen te worden naar aanleiding van een inzageverzoek.

In de loop der tijd zijn specifieke technologieën ontstaan om gegevens te verzamelen en te analyseren, zoals het koppelen van bestanden en datamining. Deze technieken zijn ook bruikbaar voor het ontsluiten van informatie naar aanleiding van de toepassing van het inzagerecht, waarbij het accent ligt op het vaststellen van de informatiebehoefte met betrekking tot de persoonsgegevens vastgelegd in elektronische bestanden. Het voordeel van het gebruik van bovenstaande technieken is dat er een standaardmethodiek wordt ontwikkeld die bij een inzageverzoek op een adequate wijze de benodigde informatie kan verschaffen.