

## **CBP Richtsnoeren**

### **ACTIEVE OPENBAARMAKING VAN PERSOONSGEGEVENS**

Consultatiedocument

# Inhoudsopgave

Inleiding .....	4
Stroomschema .....	9
1 Basisbeginselen van de bescherming van persoonsgegevens bij actieve openbaarmaking .....	11
1.1 Inleiding .....	11
1.2 Op wie legt de wet verplichtingen? De verantwoordelijke .....	12
1.3 Wat is een persoonsgegeven? .....	12
1.3.1 Iedere informatie .....	13
1.3.2 Betreffende een persoon .....	13
1.3.3 Direct of indirect identificerend .....	14
1.4 Wanneer is een gegeven géén persoonsgegeven? .....	14
1.5 Anonieme of pseudonieme gegevens .....	15
1.6 Wat is een <i>bijzonder</i> persoonsgegeven? .....	16
1.6.1 Uitzonderingen op het verbod om bijzondere persoonsgegevens te publiceren .....	17
1.7 Internationaal kader .....	18
2 Verplichtingen van de verantwoordelijke .....	19
2.1 Inleiding .....	19
2.2 Legitieme doeleinden .....	19
2.3 Verdere verwerking .....	20
2.3.1 Verder gebruik van persoonsgegevens .....	21
2.3.2 Geheimhoudingsplicht .....	22
2.4 Toestemming vragen of noodzaak kunnen aantonen .....	22
2.4.1 Toestemming .....	22
2.4.2 Noodzaak .....	23
2.5 Informatieplicht .....	27
2.5.1 Omvang informatieplicht .....	27
2.5.2 Privacyverklaring .....	28
2.5.3 Identiteitsvermelding .....	28
2.6 Meldingsplicht .....	28
2.7 Kwaliteit .....	29
2.7.1 Beperkt bewaren .....	29
2.7.2 Toereikend, ter zake dienend en niet bovenmatig .....	30
2.8 Beveiliging .....	31
2.9 Verwijderen van onrechtmatigheden .....	33
3 Rechten van betrokkenen .....	34
3.1 Inleiding .....	34
3.2 Inzage .....	34
3.3 Correctie en verwijdering .....	35
3.4 Recht van verzet .....	35
3.5 Besluiten in de zin van de Awb .....	35
4 Handhaving en de rol van het CBP .....	36

4.1	Inleiding .....	36
4.2	Maatregelen door betrokkenen .....	36
4.2.1	Rechtsbescherming onder de Wbp .....	36
4.2.2	Andere rechtsmiddelen voor betrokkenen .....	36
4.3	Handhaving door het CBP .....	36
4.3.1	Bemiddeling, klachtbehandeling en ambtshalve onderzoek .....	37
4.3.2	Bestuursdwang en last onder dwangsom .....	37
4.3.3	Strafrechtelijke handhaving .....	37
4.3.4	Internationaal toezicht .....	37
5	Managementsamenvatting .....	38
	Regels .....	38
	Voorafgaand aan publicatie .....	38
	Tijdens publicatie .....	38
	Volgend op publicatie.....	39
	Sancties.....	39
Bijlage 1	.....	40
	Raad van Europa.....	40
	Artikel 29 Werkgroep.....	40
Bijlage 2 – Wettelijke verplichtingen tot actieve openbaarmaking	.....	42
	Hergebruik .....	47

## Inleiding

De overheid kent een lange traditie van openbaarheid van bepaalde gegevensbestanden, zoals het kadaster en het handelsregister.

De afgelopen decennia is er daarnaast ook steeds meer aandacht voor openbaarheid van bestuur. De doelstelling daarvan is uiteindelijk het bevorderen van een goede en democratische bestuursvoering. Om dat te bereiken is transparantie van het openbaar bestuur een belangrijk middel. Die wordt op haar beurt weer goeddeels bereikt door het openbaar maken van overheidsinformatie.

Tot eind jaren negentig ging het bij zowel specifieke openbaarheid – in de vorm van bijvoorbeeld openbare registers – als bij algemene openbaarheid – op basis van de Wet openbaarheid bestuur (Wob) – vooral om *passieve* openbaarmaking, dat wil zeggen: informatieverschaffing *op verzoek*. Voorbeelden zijn bij specifieke openbaarheid het op verzoek toezenden van een uittreksel uit het handelsregister, en bij algemene openbaarheid het op verzoek verlenen van inzage in of toezenden van bepaalde bij de overheid berustende informatie.

Het afgelopen decennium is de aandacht echter steeds meer verschoven naar *actieve openbaarmaking*, dat wil zeggen: informatieverschaffing uit eigener beweging. Sinds begin jaren negentig draagt art. 8 Wob bestuursorganen op om uit eigen beweging informatie te verschaffen over hun beleid, waaronder de voorbereiding en uitvoering ervan, zodra dat in het belang is van een goede en democratische bestuursvoering. Actief openbaar maken kan onder meer door de betreffende informatie ter inzage te leggen, door haar op een gegevensdrager beschikbaar te stellen of door haar op internet te publiceren.

Transparantie van het openbaar bestuur is onmisbaar voor een goed functionerende democratische samenleving, en openbaarheid van overheidsinformatie is daarom een fundamentele bouwsteen van het informatiebeleid van de overheid. Bij veel van de gegevens die de overheid openbaar maakt gaat het echter geheel of gedeeltelijk om *persoonsgegevens*. Er kan in dat geval een conflict ontstaan met de bescherming van de persoonlijke levenssfeer in het algemeen, en de bescherming van persoonsgegevens in het bijzonder.

Eerbiediging van de persoonlijke levenssfeer wordt beschouwd als een essentiële voorwaarde voor een menswaardig bestaan en als een van de grondslagen van onze rechtsorde. Eenieder heeft recht op bescherming tegen de ongebreidelde vergaring, bewerking en verspreiding van zijn persoonsgegevens. Daarom stelt de wet grenzen aan actieve openbaarmaking.

Over de verhouding tussen de openbaarheid van bestuur en de bescherming van persoonsgegevens – en de daarbij te maken afwegingen – is al veel gezegd en geschreven. Dat is echter bijna allemaal gebaseerd op een context van *passieve* openbaarmaking. Bij de meeste wetten, jurisprudentie en commentaren is geen rekening gehouden met de stormachtige opkomst van het *World Wide Web* het afgelopen decennium en het daarmee samenhangende fenomeen van *actieve openbaarmaking via internet*.

Wat is er dan zo anders aan actieve openbaarmaking via internet dat speciale aandacht voor dat fenomeen rechtvaardigt? Dat zit hem vooral in de verstrekkende *gevolgen* die actieve openbaarmaking via internet kan hebben. Publicatie op internet leidt er vaak toe dat gegevens wereldwijd onbeperkt beschikbaar komen. Als de betreffende pagina's indexeerbaar zijn voor zoekmachines zijn de gegevens bovendien ook nog eens zeer eenvoudig te vinden. Daardoor kunnen derden op ongekeerde schaal over personen gegevens verzamelen waarvan zij het bestaan of de inhoud niet konden vermoeden. Zij kunnen die informatie in een andere context opnieuw publiceren of er gebruik van maken met het oog op 'cross searching', het opstellen van profielen en zelfs datawarehousing en data-mining. Zulk verder gebruik kan onrechtmatig zijn en voor doeleinden die inbreuk maken op de persoonlijke levenssfeer van betrokkenen. Op het bestuursorgaan dat de gegevens openbaar maakt rust de verantwoordelijkheid en de verplichting om dergelijk onrechtmatig gebruik te voorkomen. Dat betekent eerst en vooral: niet meer gegevens openbaar

maken dan noodzakelijk is gelet op het doel dat met de openbaarmaking wordt beoogd. Ook dient de verantwoordelijke de gegevens adequaat te beveiligen tegen onrechtmatig verder gebruik. Dat kan in een aantal gevallen door de gegevens wel openbaar te maken, maar te voorkomen dat de achterliggende database 'leeggetrokken' kan worden en ook zoekmachines geen toegang tot de gegevens te bieden.

In de kaders bij deze inleiding staan enkele voorbeelden van misbruik dat gemaakt kan worden van actief openbaar gemaakte persoonsgegevens. Ook elders in de richtsnoeren zijn die te vinden, bijvoorbeeld in het kader "Geen handtekening publiceren op internet" in paragraaf 2.8.2.

Hoofregel van de Wet bescherming persoonsgegevens (hierna: Wbp) is dat iedereen die persoonsgegevens openbaar maakt zélf verantwoordelijk is voor de naleving van de wet. Bestuursorganen die voornemens zijn gegevens over personen actief openbaar te maken, dienen dus zelf voorafgaand aan de publicatie te beoordelen of dat wel is toegestaan, en zo ja, in welke vorm dat kan en aan welke voorwaarden zij daarbij moeten voldoen.

Met deze richtsnoeren wil het College bescherming persoonsgegevens (hierna: CBP) het eenvoudiger maken om dat te beoordelen. Dat is in het belang van degenen die actief persoonsgegevens openbaar maken en in het belang van de mensen over wie (mogelijk) gegevens openbaar worden gemaakt.

Deze richtsnoeren behandelen de hoofdlijnen van de beoordeling van actieve openbaarmaking door de overheid, onder de geldende privacywetgeving en jurisprudentie.<sup>1</sup> Openbaarmaking kan ook uit anderen hoofde dan privacybescherming onrechtmatig zijn, bijvoorbeeld omdat ze in strijd is met de Auteurswet. De handvatten in deze richtsnoeren zijn beperkt tot de toelaatbaarheid van openbaarmaking onder de geldende privacywetgeving. In deze richtsnoeren wordt dus niet ingegaan op de rechtmatigheid van openbaarmaking in het licht van andere wetgeving.

De richtsnoeren behandelen veel van de belangrijkste regels op het gebied van de bescherming van persoonsgegevens maar bevatten geen uitputtende beschrijving van alle bestaande wettelijke bepalingen en jurisprudentie. De voorbeelden die in deze richtsnoeren zijn opgenomen, dienen alleen ter illustratie van de manier waarop het CBP een specifieke bepaling uit de Wbp toepast bij de beoordeling van actieve openbaarmaking. Openbaarmaking in een vorm die niet bij wijze van voorbeeld in deze richtsnoeren is opgenomen, kan toch in strijd zijn met de Wbp.

Bij de beoordeling van een vorm van actieve openbaarmaking die vergelijkbaar is met een voorbeeld kunnen ook andere dan de besproken Wbp-bepalingen een rol spelen. Ook indien een concreet (soort) publicatie veel lijkt op een voorbeeld, dient men erop bedacht te zijn dat de definitieve beoordeling alleen gemaakt kan worden met inachtneming van alle omstandigheden van het individuele geval en dat de beoordeling daarom anders kan uitpakken.

Rechterlijke uitspraken kunnen naast wetswijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding vormen tot aanvulling of herziening van deze richtsnoeren.

Actieve openbaarmaking kan op diverse manieren gebeuren. De vanuit het oogpunt van bescherming van persoonsgegevens meest relevante manier is: publicatie op internet. De term *actieve openbaarmaking* wordt in deze richtsnoeren dan ook gebruikt in die beperktere betekenis.<sup>2</sup> Dat laat onverlet dat de bescherming van persoonsgegevens nu juist

---

<sup>1</sup> Het juridisch kader bestaat voornamelijk uit de Wet bescherming persoonsgegevens (Wet van 6 juli 2000, Stb. 302), jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM), het Europees Hof van Justitie (HvJEG) en relevante interpretaties van de Artikel 29-werkgroep, het samenwerkingsverband van toezichthouders op het gebied van bescherming van persoonsgegevens in de Europese Unie (EU). Waar relevant komt ook algemene Nederlandse jurisprudentie aan de orde, evenals uitspraken van het CBP zelf. Twee in het bijzonder relevante internationale documenten worden samengevat in de bijlage.

<sup>2</sup> Tenzij uit de context duidelijk is dat het gaat over actieve openbaarmaking in bredere zin.

met zich meebrengt dat de verantwoordelijke telkens een afweging moet maken of publicatie op internet een acceptabele wijze van actieve openbaarmaking is.

#### PERSOONSgegevens NIET VOGELVRIJ

In zijn advies van 15 mei 2007 over de Wet algemene bepalingen omgevingsrecht (Wabo)<sup>3</sup> schreef het CBP: *Bezinning is nodig op de vraag waarom openbaarheid zonder meer openbaar op internet zou inhouden. Persoonsgegevens die via internet worden gepubliceerd, kunnen door een onbekend aantal internetgebruikers uit de hele wereld voor eigen doeleinden worden verzameld en verwerkt, ook jaren nadat de oorspronkelijke publicatie van internet is verdwenen. Het voordeel van digitaliseren mag niet omslaan in het nadeel dat persoonsgegevens vogelvrij zijn op internet.*

Het CBP heeft eind vorig jaar richtsnoeren gepubliceerd voor de publicatie van persoonsgegevens op internet.<sup>4</sup> Uit de aard der zaak is er sprake van een behoorlijke mate van overlap tussen die richtsnoeren en de onderhavige. Anderzijds gaan de richtsnoeren voor publicatie van persoonsgegevens op internet in op een aantal onderwerpen die hier niet of slechts zijdelings belicht kunnen worden. Bestuursorganen die actief persoonsgegevens openbaar maken en bepaalde vragen niet in deze richtsnoeren geadresseerd zien, worden daarom verwezen naar de CBP richtsnoeren voor de publicatie van persoonsgegevens op internet.

Deze richtsnoeren treden in werking met ingang van ... .. 2008, zijnde de datum van publicatie in de Staatscourant.

#### PUBLICATIE VAN GEGEVENS OVER VERLEENDE LANDBOUWSUBSIDIES

In 2005 kreeg het ministerie van LNV een verzoek van de Evert Vermeer-stichting om op grond van de Wob informatie te verstrekken over subsidies verleend in het kader van het Gemeenschappelijk landbouwbeleid van de EU. Naar aanleiding hiervan besloot het ministerie in 2006 om deze subsidies voortaan actief openbaar te maken. In verband met het risico van onrechtmatig verder gebruik werden echter niet alle gegevens op internet geplaatst, en werden de wél openbaar gemaakte gegevens beveiligd. De functionaris voor de gegevensbescherming van LNV schrijft hierover in zijn jaarverslag over 2006 het volgende (blz. 13–14):

[Noot voor de vormgever: om te voorkomen dat de onderstaande tekst aan het CBP wordt toegeschreven dient deze duidelijk afwijkend te worden vormgegeven.]

“Met ingang van mei 2006 worden gegevens over verleende subsidies in het kader van het Gemeenschappelijk Landbouwbeleid (GLB) jaarlijks openbaar gemaakt en op de website van LNV geplaatst. Hierbij worden ook de persoonsgegevens van de ontvangers vermeld. Het gaat hierbij niet om openbaarmaking op verzoek, maar om actieve openbaarmaking. Daarbij is wat meer beleidsruimte wat betreft de afweging welke gegevens in welke vorm openbaar zullen worden gemaakt.

*Naw-gegevens openbaar, registratienummers niet*

Evenals in 2005 worden vanaf 2006 de naam-, adres- en woonplaatsgegevens (naw-gegevens) actief openbaar gemaakt bij de uitgekeerde bedragen. In 2005 gebeurde dit ook al, op verzoek van de Evert Vermeer Stichting. Bij de actieve open-

<sup>3</sup> CBP, brief aan de leden van de vaste Kamercommissie voor VROM, z2007-00304, 15 mei 2007, [http://www.cbweb.nl/documenten/med\\_20070515\\_wabo](http://www.cbweb.nl/documenten/med_20070515_wabo).

<sup>4</sup> *Publicatie van persoonsgegevens op internet*. CBP Richtsnoeren, december 2007. Gepubliceerd in de Staatscourant van 11 december 2007.

baarmaking van de GLB-subsidiegegevens in 2006 werden echter niet meer de registratienummers van de ontvangers (de BRS-nummers) vermeld. Aan het vermelden van de BRS-nummers kleefte het nadeel dat derden zich hierdoor toegang kunnen verschaffen tot gegevens van anderen, die beschermd moeten worden. Ten tijde van de publicatie in 2005 heeft de Dienst Regelingen de klantidentificatie tijdelijk moeten verscherpen om misbruik te voorkomen.

#### *Voorzieningen tegen oneigenlijk gebruik*

De FG heeft aan de minister voorgesteld om, wanneer persoonsgegevens worden gepubliceerd, de wijze van publicatie zodanig in te richten dat het register zo min mogelijk uitnodigt tot onbedoeld gebruik, of dat gebruik überhaupt niet mogelijk maakt. Er zijn voorzieningen tegen oneigenlijk gebruik nodig. Voorbeelden van oneigenlijk gebruik zijn: raadpleging uit pure nieuwsgierigheid naar persoonlijke omstandigheden, commerciële doeleinden zoals geadresseerde reclame, identiteitsdiefstal en andere vormen van hinder of criminaliteit. Wanneer persoonsgegevens integraal en onbeveiligd op internet worden gepubliceerd, bestaat een groter risico voor de bescherming van de veiligheid of de persoonlijke levenssfeer van betrokkenen. De minister besloot op 23 februari 2006 dat een voorziening zal worden getroffen voor het beperken van het risico van oneigenlijk gebruik van de gegevens voor direct marketing doeleinden. De secretaris-generaal besloot in april tot diverse concrete voorzieningen.

#### *Concreet beveiligingsrisico*

In oktober 2006 probeerde een organisatie uit Denemarken met regelmaat de gehele inhoud van deze database te downloaden. Daardoor ontstaat een dreiging voor de website en voor de bescherming van de belangen van individuele personen. De secretaris-generaal stemde in met het treffen van aanvullende technische voorzieningen, en met het voorstel dat bij een "doorbraak" de database van het internet zal worden gehaald."

### **Gebruik van milieugegevens voor politieke doeleinden**

Als onderdeel van zijn campagne voor herverkiezing voor de gemeenteraad stuurt een lokale politicus een brief aan een aantal inwoners van de gemeente. De adressen van deze inwoners haalt hij uit een openbaar bestand met milieu-informatie. Is dit verder gebruik toegestaan?

Het openbare bestand met milieu-informatie vindt zijn oorsprong in Richtlijn 2003/4/EG van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie, die strekt tot implementatie van het Verdrag van Aarhus. Deze Richtlijn schept verplichtingen voor de lidstaten tot zowel het op verzoek verstrekken als het actief openbaar maken van milieu-informatie. Waar het persoonsgegevens betreft wordt daarbij expliciet Richtlijn 95/46/EG als toetsingskader genoemd voor de afweging wel of niet openbaar maken. Er is wel een uitzondering: emissiegegevens dienen altijd verstrekt te worden. Richtlijn 2004/03 is op zijn beurt geïmplementeerd in (onder meer) de Wet milieubeheer.

De ratio achter deze regels is in essentie te vinden in de eerste overweging bij Richtlijn 2004/03/EG: *Een verruimde toegang van het publiek tot milieu-informatie en verspreiding van die informatie dragen bij tot een verhoogd milieubewustzijn, een vrije gedachteswisseling, een doeltreffender deelneming van het publiek aan de milieubesluitvorming en, uiteindelijk, tot een beter milieu.*

Uit het internationale kader en de Wbp volgt dat het verdere gebruik van deze gegevens voor politieke doeleinden in het algemeen niet is toegestaan, aangezien dit zal falen op het vereiste van verenigbaarheid: het voor zich trachten te winnen van

kiezers – zelfs op basis van milieupolitieke argumenten – kan niet geacht worden bij te dragen aan verbetering van het milieu in de zin van de Richtlijn, en ligt ook te ver van die doelstelling af. Merk op dat het hierbij niet relevant is of het gaat om emissie-informatie of andere milieu-informatie. Weliswaar hoeft bij het publiceren van emissie-informatie geen rekening te worden gehouden met de persoonlijke levenssfeer, maar het gaat hier niet over het *publiceren* van de informatie, maar over het *verdere gebruik* ervan.

## Stroomschema

Bent u een bestuursorgaan of andere overheidsinstelling die actief gegevens openbaar maakt? (zie de inleiding en § 1.2)	NEE ▶	Deze richtsnoeren zijn niet op u van toepassing. (Zie de laatste alinea van Bijlage 2 als u overheidsgegevens hergebruikt.) In het hoofdstuk 'Rechten van betrokkenen' kunt u lezen wat uw rechten zijn als gegevens over u tegen uw zin actief openbaar gemaakt worden.
JA ▼		
Maakt u actief gegevens over (levende) natuurlijke personen openbaar? (zie de §§ 1.3 t/m 1.5)	NEE ▶	De Wbp is alleen van toepassing op gegevens die herleidbaar zijn naar (levende) natuurlijke personen. Deze richtsnoeren zijn niet op de door u openbaar gemaakte gegevens van toepassing.
JA ▼		
Gaat het om strafrechtelijke gegevens, of gegevens over iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging? (zie § 1.6)	JA ▶	Openbaarmaking is niet toegestaan, tenzij u daartoe expliciet wettelijk verplicht bent, de betroffene persoon uitdrukkelijke toestemming heeft gegeven of deze de betreffende informatie duidelijk zelf openbaar heeft gemaakt.
NEE ▼		
Bevatten de gegevens wettelijk voorgeschreven identificatienummers, zoals het BSN? (zie § 1.6.2)	JA ▶	Openbaarmaking van wettelijk voorgeschreven identificatienummers is niet toegestaan.
NEE ▼		
Rust op u een expliciete wettelijke verplichting (niet de Wob) om de gegevens actief openbaar te maken, of is de openbaarmaking noodzakelijk <sup>5</sup> voor de goede vervulling van een u opgedragen publiekrechtelijke taak, of heeft de betrokkene toegestemd in openbaarmaking? (zie § 2.4 en Bijlage 2)	NEE ▶	U mag geen persoonsgegevens openbaar maken zonder rechtvaardigingsgrond uit artikel 8 Wbp. In uitzonderlijke gevallen kan een beroep worden gedaan op artikel 8 onder f Wbp, gerechtvaardigd belang dat zwaarder weegt dan het privacybelang van de betrokkenen (zie § 2.4.2.3).
JA ▼		
Heeft u voldoende maatregelen genomen om te zorgen dat de openbaarmaking verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?	NEE ▶	Persoonsgegevens mogen alleen openbaar gemaakt worden als dat verenigbaar is met het doeleinde waarvoor ze verzameld zijn. Verenigbaarheid is vaak te bereiken door het scheppen van de juiste waarborgen.

<sup>5</sup> Het noodzakelijkheids criterium houdt een afweging van belangen in.

Heeft u de betrokken personen geïnformeerd over de openbaarmaking? (zie § 2.5)

JA ▼

NEE ▶

Indien u gegevens openbaar maakt dient u de betrokken personen daarover vooraf te informeren.

Heeft u het openbaar maken van de gegevens gemeld bij het CBP? (zie § 2.6)

JA ▼

NEE ▶

Tenzij het gaat om een bij wet ingestelde openbaar register dient u de openbaarmaking te melden bij het CBP.

Heeft u voldoende maatregelen getroffen om de kwaliteit (waaronder de actualiteit) van de openbaar gemaakte gegevens voldoende te kunnen garanderen? (zie § 2.7)

JA ▼

NEE ▶

U moet zorgen dat de kwaliteit van de openbaar gemaakte gegevens voldoende is en blijft.

Heeft u de gegevens afdoende beveiligd? Zijn ze in het bijzonder afgeschermd voor indexing door zoekmachines en bulkopvragingen? (zie § 2.8)

JA ▼

NEE ▶

U dient de openbaar gemaakte gegevens op adequate wijze te beveiligen.

Stelt u de betrokken burgers in staat om hun rechten op onder meer inzage, verzet, correctie en verwijdering uit te oefenen? (zie Hoofdstuk 3)

JA ▼

NEE ▶

U dient burgers in staat te stellen om hun rechten onder de Wbp uit te oefenen.

U mag de gegevens openbaar maken, mits u dat ook overigens op een behoorlijke en zorgvuldige wijze doet. (zie art. 6 Wbp)

# 1 Basisbeginselen van de bescherming van persoonsgegevens bij actieve openbaarmaking

## 1.1 Inleiding

De Wob vormt de leidraad voor overheden die gegevens – passief of actief – openbaar maken. Als het gaat om *persoonsgegevens* is er daarnaast nog een tweede leidraad, namelijk de regelgeving ter bescherming van persoonsgegevens. Beide regelstelsels hebben een ingewikkelde en soms onduidelijke verwevenheid met elkaar.

De Europese privacyrichtlijn 95/46/EG (hierna: de Richtlijn) vormt het verplichte kader voor de bescherming van persoonsgegevens. Dat betekent dat openbaarmaking van persoonsgegevens op basis van de Wob slechts mogelijk is binnen de grenzen van de Richtlijn. Dit heeft gevolgen voor de interpretatie van de uitzonderingsgronden in de Wob die de persoonlijke levenssfeer betreffen. Dat zijn artikel 10 lid 1 onder d Wob<sup>6</sup> en artikel 10 lid 2 onder e Wob<sup>7</sup>. In deze uitzonderingsgronden dient het hele stelsel van voorwaarden en waarborgen uit de Richtlijn<sup>8</sup> te worden ingelezen. Dat kan bijvoorbeeld met zich mee brengen dat een bestuursorgaan persoonsgegevens die het in het kader van actieve openbaarmaking op internet gepubliceerd heeft weer moet verwijderen, bijvoorbeeld omdat de openbaarmaking gelet op het beoogde doel niet langer nodig is.<sup>9</sup>

Het voorgaande is slechts relevant voor zover de Wob een bestuursorgaan *verplicht* tot het openbaar maken van persoonsgegevens. Verderop in deze richtsnoeren<sup>10</sup> wordt besproken dat de Wob in het algemeen niet kan worden geacht een verplichting tot het actief openbaar maken van persoonsgegevens *op internet* in te houden. Ook andere wetgeving bevat slechts incidenteel de verplichting tot openbaarmaking van persoonsgegevens op internet, en doorgaans rust die verplichting dan op een specifiek bestuursorgaan. Voor actieve openbaarmaking van persoonsgegevens op internet heeft een bestuursorgaan daarom in het algemeen geen rechtvaardigingsgrond in artikel 8 onder c Wbp.

Iedere verwerking van persoonsgegevens behoeft een rechtvaardigingsgrond in artikel 8 Wbp.<sup>11</sup> Nu dat zelden artikel 8 onder c Wbp blijkt te kunnen zijn, is de meest in aanmerking komende rechtvaardigingsgrond artikel 8 onder e Wbp: de openbaarmaking is noodzakelijk voor de goede uitvoering van een publiekrechtelijke taak van het desbetreffende bestuursorgaan. De term “noodzakelijk” houdt een afweging in van het belang van de openbaarmaking enerzijds en het privacybelang van de betrokkenen anderzijds. Een bestuursorgaan dat het voor de goede uitvoering van een publiekrechtelijke taak die het heeft nodig acht persoonsgegevens actief openbaar te maken door middel van publicatie op internet, dient zich af te vragen of dit niet ook mogelijk is via een minder ingrijpend middel (‘subsidiariteit’) en zo nee, of het middel überhaupt wel in verhouding staat tot het daarmee te bereiken doel (‘proportionaliteit’).<sup>12</sup> Zelfs als de openbaarmaking duidelijk bijdraagt aan het goed vervullen van een publiekrechtelijke taak kan het dus zo zijn dat

---

<sup>6</sup> “Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit: ... d. persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.”

<sup>7</sup> “Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen: ... e. de eerbiediging van de persoonlijke levenssfeer.”

<sup>8</sup> En daarmee voor een groot deel de Wbp.

<sup>9</sup> Zie § 2.7.1.

<sup>10</sup> In § 2.4.2.2.

<sup>11</sup> Zie § 2.4.

<sup>12</sup> Zie § 2.4.2.1.

de conclusie moet luiden dat voor een andere vorm van openbaarmaking moet worden gekozen, of dat openbaarmaking geheel achterwege dient te blijven.

Actief openbaar gemaakte persoonsgegevens moeten op dezelfde zorgvuldige wijze worden verwerkt als passief openbaar gemaakte persoonsgegevens. Sterker nog: gelet op de extra risico's waarmee actieve openbaarmaking op internet gepaard gaat, dient daarbij extra terughoudendheid te worden betracht.

De Wet bescherming persoonsgegevens is van toepassing op 'de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens',<sup>13</sup> en dus op elke openbaarmaking<sup>14</sup> van persoonsgegevens via gegevensdragers zoals USB-sticks of CD-ROMs of via netwerken, zoals internet.<sup>15</sup> Het gaat hierbij zowel over het openbaar maken van persoonsgegevens als zodanig als over het openbaar maken van documenten of bestanden die (onder meer) persoonsgegevens bevatten. Ieder bestuursorgaan dat persoonsgegevens openbaar maakt dient te voldoen aan de verplichtingen die de wet oplegt. Deze zijn: het behoorlijk en zorgvuldig te werk gaan, transparantie, doelbinding, rechtvaardigingsgrond, kwaliteit en evenredigheid, informatierecht van burgers, beveiliging en beperking van doorgifte naar landen buiten de EU.

Artikel 1 van de Wbp bevat definities van de begrippen die in de wet worden gehanteerd. Niet alle begrippen zijn even relevant voor het beoordelen van actieve openbaarmaking. Hieronder volgen de belangrijkste.

## 1.2 Op wie legt de wet verplichtingen? De verantwoordelijke

Met de term 'verantwoordelijke' wordt in deze richtsnoeren degene aangeduid die onder de Wbp verantwoordelijk is voor het actief openbaar maken persoonsgegevens. Volgens de wet is de verantwoordelijke *de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*. Aangezien het hier gaat over het actief openbaar maken van bij de overheid berustende gegevens, zal de verantwoordelijke in vrijwel alle gevallen een bestuursorgaan zijn.

Met de term 'betrokkene' wordt de persoon bedoeld wiens persoonsgegevens worden verwerkt.

## 1.3 Wat is een persoonsgegeven?

De Wbp kent een ruime definitie van persoonsgegevens. In artikel 1 sub a Wbp wordt een persoonsgegeven gedefinieerd als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. De omschrijving is letterlijk overgenomen van arti-

---

<sup>13</sup> De wet is ook van toepassing op niet geautomatiseerde verwerkingen, zoals papieren dossiers, maar alleen als de gegevens opgenomen zijn of worden in een bestand, dat wil zeggen een gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

<sup>14</sup> Hierop bestaan wel enkele uitzonderingen. In de eerste plaats is de Wbp niet van toepassing voor enkele specifieke overheidsterreinen genoemd in artikel 2 Wbp. Zie hiervoor § 2.4.2.1. Daarnaast zijn er drie soorten gegevensgebruik waarop de Wbp niet of slechts gedeeltelijk van toepassing is. Dat zijn: verwerkingen voor persoonlijk of huishoudelijk gebruik, gebruik voor uitsluitend journalistieke, artistieke of literaire doeleinden en gebruik voor historische, wetenschappelijke of statistische doeleinden. Van de eerste twee soorten zal bij actieve openbaarmaking nooit sprake zijn. Actieve openbaarmaking voor historische, wetenschappelijke of statistische doeleinden is denkbaar. Zie voor de eisen die de Wbp daaraan stelt paragraaf 1.7.3 van de Richtsnoeren van het CBP voor publicatie van persoonsgegevens op internet.

<sup>15</sup> Memorie van toelichting bij de Wbp, Kamerstukken II, 28 509, 3 (hierna: MvT), blz 71: 'Zodra informatie digitaal is vastgelegd is er in ieder geval sprake van geautomatiseerde verwerking van gegevens. In een geautomatiseerd systeem is immers het zoeken naar digitale gegevens mogelijk. (...) Het feit dat langs geautomatiseerde weg geluid- of beeldvergelijking van digitaal vastgelegde informatie over iemand onvergelykbaar veel sneller en nauwkeuriger kan plaatsvinden dan wanneer dit handmatig zou moeten geschieden, rechtvaardigt een aangescherpt juridisch regime.'

kel 2 van het Europees Dataverdrag.<sup>16</sup> De Europese privacyrichtlijn 95/46/EG waarop de Wbp is gebaseerd, geeft een iets uitgebreidere omschrijving.

De Richtlijn geeft in artikel 2 onder a als definitie van persoonsgegevens:

*iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.*

Hoewel het tweede deel van de Europese definitie, de uitleg over specifieke elementen die iemand identificeerbaar maken, niet is overgenomen in de Wbp, maakt de memorie van toelichting bij de Wbp duidelijk dat de Wbp het zelfde uitgangspunt hanteert ten aanzien van indirect identificerende gegevens.

*Allereerst is voor het begrip 'persoonsgegeven' relevant of de gegevens informatie over een persoon bevatten. In veel gevallen, zoals bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen, zal dit uit de aard van de gegevens voortvloeien. In andere gevallen zal mede aandacht moeten worden besteed aan de context waarin het gegeven wordt vastgelegd en gebruikt. Als gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt. Het (maatschappelijk) gebruik dat van gegevens wordt gemaakt is dus medebepalend voor de beantwoording van de vraag of sprake is van een persoonsgegeven.<sup>17</sup>*

De Artikel 29-werkgroep van samenwerkende toezichthouders op de gegevensbescherming in de EU heeft vorig jaar in een opinie<sup>18</sup> de verschillende onderdelen van de definitie van persoonsgegevens nader uitgewerkt. Het gaat om de begrippen 'iedere informatie', 'betreffende een natuurlijk persoon' en 'direct of indirect herleidbaar'.

### **1.3.1 Iedere informatie**

De werkgroep benadrukt dat 'iedere informatie' zowel objectieve als subjectieve gegevens omvat, ongeacht of ze juist of bewezen zijn. Denk aan een waardeoordeel als 'De aanvrager van deze vergunning heeft dubieuze connecties'.<sup>19</sup>

Ook foto's, video- en geluidsopnamen van herkenbare natuurlijke personen zijn persoonsgegevens.<sup>20</sup>

### **1.3.2 Betreffende een persoon**

Om te bepalen of een gegeven betrekking heeft op een persoon, moet volgens de Artikel 29-werkgroep één van de volgende drie elementen aanwezig zijn: een inhoudelijk element, een doelelement of een resultaattelement.

Een inhoudelijk element betekent dat het om informatie gaat over een persoon, ongeacht het doeleinde van de verantwoordelijke of het resultaat voor die persoon, zoals een verleende vergunning betrekking heeft op de aanvrager of zoals de gegevens in een cliëntenbestand van een instantie betrekking hebben op de cliënt.

---

<sup>16</sup> Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 1981, Trb. 1988, 7.

<sup>17</sup> Memorie van toelichting bij de Wbp, Kamerstukken II, nr 25 892, nr. 3, blz 46.

<sup>18</sup> Opinion 4/2007 on the concept of personal data van de Artikel 29-werkgroep, aangenomen op 20 juni 2007.

<sup>19</sup> Opinion 4/2007, blz. 6.

<sup>20</sup> Richtlijn 95/46/EG, overweging 14: 'overwegende dat, gezien het belang van de in het kader van de informatiemaatschappij aan de gang zijnde ontwikkelingen inzake de technieken voor het opvangen, doorsturen, manipuleren, registreren, bewaren of mededelen van geluid- en beeldgegevens betreffende natuurlijke personen, deze richtlijn ook van toepassing zal moeten zijn op verwerkingen die op deze gegevens betrekking hebben.'

Ook de aanwezigheid van een doelelement kan ertoe leiden dat gegevens als persoonsgegevens worden beschouwd. Daar is sprake van als de gegevens (waarschijnlijk) gebruikt worden met het doel om iemand op een bepaalde manier te behandelen of diens status of gedrag te beoordelen of te beïnvloeden. Dat kan het geval zijn als een uitkeringsinstantie informatie verzamelt over het water- en energiegebruik in huishoudens met het oog op het verkrijgen van aanwijzingen van fraude.

Als er geen inhoudelijk of doelelement is, kunnen gegevens toch persoonsgegevens zijn, als het gebruik ervan waarschijnlijk invloed heeft op de rechten en belangen van een persoon, zodanig dat die persoon daardoor anders wordt behandeld. Dat kan het geval zijn als de overheid ten behoeve van rekeningrijden met behulp van GPS de locaties van voertuigen op bepaalde wegen in de gaten houdt. Hoewel het systeem gericht is op het verwerken van gegevens over de routes van voertuigen, kunnen de gegevens ook gebruikt worden om de bestuurders te beoordelen.<sup>21</sup>

### 1.3.3 Direct of indirect identificerend

Gegevens kunnen direct of indirect identificerend zijn.

Het bekendste direct identificerende gegeven is de combinatie van voornaam, achternaam en adres. De bekendste indirect identificerende gegevens zijn (e-mail)adres, telefoonnummer, kenteken en de combinatie postcode/huisnummer.<sup>22</sup> Andere indirect identificerende gegevens zijn gegevens over iemands eigenschappen, opvattingen of gedragingen, waarmee die persoon wordt onderscheiden van andere personen. Bijvoorbeeld: de directeur van een met name genoemde onderneming.

Bij het vaststellen of een gegeven een indirect identificerend persoonsgegeven is, is van belang of de identiteit van de persoon er redelijkerwijs, zonder onevenredige inspanning, mee kan worden vastgesteld. Het is niet doorslaggevend of het identificeren daadwerkelijk plaatsvindt. Deze opvatting komt voort uit overweging 26 bij de privacyrichtlijn: *Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, dat om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren. (...). Herleidbaarheid tot een natuurlijk persoon, voorzover die redelijkerwijs door een derde kan worden bewerkstelligd, is dus voldoende.*

## 1.4 Wanneer is een gegeven géén persoonsgegeven?

Gegevens over organisaties, zoals bedrijven of stichtingen, zijn geen persoonsgegevens in de zin van de Wbp. De wet is wel weer van toepassing op bedrijven als het gegeven herleidbaar is naar een persoon, zoals bij een eenmanszaak, of als het over de individuele bestuurders gaat van een onderneming of stichting. Bij actieve openbaarmaking van bedrijfsgegevens zal het in veel gevallen niet haalbaar zijn om onderscheid te maken tussen bedrijfsgegevens die wél en bedrijfsgegevens die géén persoonsgegevens zijn. In zulke gevallen vereist de wet dat alle betreffende gegevens behandeld worden als waren zij persoonsgegevens.

De Wbp is evenmin van toepassing op gegevens die betrekking hebben op personen die overleden zijn. Als de gegevens van een overledene echter ook betrekking hebben op een nabestaande (bijvoorbeeld in het geval van informatie over een erfelijke ziekte) kan de Wbp wel van toepassing zijn.

---

<sup>21</sup> Opinion 4/2007, blz. 9–12.

<sup>22</sup> De Registratiekamer en het CBP hebben uitspraken gedaan over telefoonnummers (oa: Registratiekamer 8 juli 1993, 93.1.002 en CBP 28 mei 2003, z2003-0480 over afscherming nummergegevens, URL: [http://www.cbpweb.nl/documenten/adv\\_z2003-0480.stm](http://www.cbpweb.nl/documenten/adv_z2003-0480.stm)); over kentekens van auto's (oa: Registratiekamer, 9 december 1996, 96-0140 trajectcontrole dmv kentekenregistratie, URL: [http://www.cbpweb.nl/downloads\\_uit/z1996-0140.pdf](http://www.cbpweb.nl/downloads_uit/z1996-0140.pdf)) en over postcodes met huisnummers (oa: Registratiekamer 21 juni 1996, 95.O.043).

Gegevens over objecten zijn over het algemeen ook geen persoonsgegevens. In grensgevallen is de context waarin van de gegevens gebruik wordt gemaakt van belang. Gegevens over objecten, zoals woonhuizen, zijn persoonsgegevens als de informatie kan worden gebruikt om de bewoners of eigenaren te beoordelen en daar consequenties aan te verbinden, zoals de hoogte van een belastingheffing.

#### PANORAMAFOTO'S VAN HUIZEN

In 2001 deed de Registratiekamer (de voorganger van het CBP) onderzoek naar het gebruik van geo-informatie.<sup>23</sup> Een bedrijf maakte digitale opnames van openbare ruimten met een beeld van 360 graden. De beelden konden doorzocht worden op gemeente, plaats, straat en huisnummer. Omdat de eigenaren en bewoners van de betrokken panden zonder onevenredige moeite konden worden geïdentificeerd en de digitale beelden onder meer door gemeenten werden gebruikt om de waarde van panden te taxeren, stelde de Registratiekamer vast dat de foto's persoonsgegevens waren, waarvoor zowel de makers als de afnemers verantwoordelijk waren in de zin van de Wbp.

### 1.5 Anonieme of pseudonieme gegevens

Geanonimiseerde gegevens zijn geen persoonsgegevens als de betrokken personen redelijkerwijs niet identificeerbaar zijn. De vraag of een gegeven daadwerkelijk anoniem is, komt met name aan de orde bij het actief openbaar maken van statistische informatie. Geaggregeerde informatie kan toch persoonsgegevens bevatten als het aantal betrokkenen klein is en er andere informatie beschikbaar is, bijvoorbeeld via zoekmachines, waardoor individuele personen toch kunnen worden geïdentificeerd.

Door pseudonimisering zijn gegevens soms geen persoonsgegevens, afhankelijk van de gekozen versleutelingsmethode. Zolang de gegevens echter zonder onevenredige inspanning herleidbaar blijven naar natuurlijke personen, door de verantwoordelijke of door een derde, moeten ze als persoonsgegevens worden behandeld.<sup>24</sup>

#### CASUSGEGEVENS INDIRECT HERLEIDBAAR

De Heij en Van de Pol beschrijven in het kader van het thema 'anonimisering van jurisprudentie'<sup>25</sup> een geval van indirecte herleidbaarheid van een anoniem gepresenteerde casus:<sup>26</sup>

"Anonimisering sluit evenwel niet uit dat de identiteit van de betrokken personen kan worden herleid en openbaar gemaakt. Dat is recentelijk nog eens gebleken in de veroordeling tot schadevergoeding van het hoofd van het WODC, prof.dr. H.G. van de Bunt, door de rechtbank Arnhem. In de pers werd de identiteit onthuld van een advocaat als mogelijk betrokkene bij georganiseerde criminaliteit. Het ging om een advocaat die commissaris was geweest bij een bedrijf en door de Ondernemingskamer was veroordeeld, omdat hij als commissaris tekort was geschoten in zijn toezichthoudende functie. Deze casus was beschreven door Van de Bunt in zijn rapportage in opdracht van de parlementaire enquêtecommissie Opsporingsmethoden. De rechtbank kwam tot het oordeel dat de omstandigheid dat de journalisten

<sup>23</sup> Registratiekamer, 16 februari 2001, z2000-1172, URL: [http://www.cbpweb.nl/documenten/uit\\_z2000-1172.stm](http://www.cbpweb.nl/documenten/uit_z2000-1172.stm).

<sup>24</sup> Zie Opinion 4/2007, blz. 18–21, voor meer voorbeelden.

<sup>25</sup> Zie daarover ook paragraaf 2.4.2.3.

<sup>26</sup> A.C.M. de Heij & U. van de Pol. "Anonimisering van jurisprudentie? Balans tussen openbaarheid van rechtspraak en privacybescherming". Trema 1999, nr. 7 (september).

de identiteit van de advocaat/commissaris hebben kunnen achterhalen aan Van de Bunt kan worden verweten.<sup>27</sup> In hoger beroep zal ongetwijfeld een belangrijk discussiepunt worden of de rechtbank hierbij de juiste maatstaf heeft gehanteerd."

Bestuursorganen die gegevens actief openbaar maken, dienen zich rekenschap te geven van de gevolgen van de vaak lange of onbepaalde termijn van een dergelijke publicatie. Door technische ontwikkelingen kan een gegeven dat op het moment van openbaarmaking geen persoonsgegeven lijkt, later toch herleidbaar worden naar een persoon. Verantwoordelijken kunnen dan vanaf dat moment worden aangesproken op grond van de Wbp.<sup>28</sup> Daarom is het van belang dat verantwoordelijken die niet in strijd met de Wbp willen handelen ervoor zorgen dat ze een beperkte, op de risico's afgestemde, termijn hanteren voor publicatie van gegevens die geen persoonsgegevens lijken en ingrijpen zodra ze merken dat gegevens alsnog herleidbaar worden naar personen.<sup>29</sup>

Zie over de termijn van openbaarmaking ook paragraaf 2.7.1.

## 1.6 Wat is een *bijzonder* persoonsgegeven?

De Wbp maakt onderscheid tussen 'gewone' en 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Ook strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag zijn bijzondere persoonsgegevens. Het begrip 'strafrechtelijke gegevens' omvat zowel informatie over veroordelingen als min of meer gegronde verdenkingen. Het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt wegens een bepaald vergrijp is ook een strafrechtelijk gegeven.

Bijzondere persoonsgegevens zijn onderworpen aan een strenger wettelijk regime dan de overige persoonsgegevens. Verwerking van bijzondere persoonsgegevens is verboden, tenzij de betrokkene daarvoor uitdrukkelijke toestemming heeft gegeven, of als de betrokkene de gegevens bewust zelf openbaar heeft gemaakt.<sup>30</sup>

In het kader bij deze paragraaf wordt toegelicht dat persoonsnummers zoals het BSN (burgerservicenummer) niet openbaar gemaakt mogen worden.

IDENTIFICATIENUMMERS NIET OPENBAAR MAKEN

<sup>27</sup> Rechtbank Arnhem 1 april 1999 (rolnummer 1996/2311). Van de Bunt is later ook in hoger beroep en in cassatie in het ongelijk gesteld. In die zaken kwam echter alleen de vraag aan de orde in hoeverre Van de Bunt aanspraak kon maken op parlementaire immuniteit. (HR 28 juni 2002, nr. C01/124, NJ 2002, 577; LJN nr. AE1544).

<sup>28</sup> Kamerstukken II, 25892, nr. 9, blz 2. Zie ook de MvT, blz 49: 'Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden, gelet op de toegenomen mogelijkheden tot herleiding'.

<sup>29</sup> Opinie 4/2007, blz 15: 'If the data are intended to be stored for one month, identification may not be anticipated to be possible during the "lifetime" of the information, and they should not be considered as personal data. However, if they are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which may make them personal data at that moment. The system should be able to adapt to these developments as they happen, and to incorporate then the appropriate technical and organisational measures in due course.'

<sup>30</sup> In de artikelen 17 t/m 23 Wbp staan een aantal uitzonderingen op het verbod beschreven, zoals het eigen gebruik van gegevens over het lidmaatschap van een politieke partij, vakbond of kerk door de desbetreffende organisatie of het gebruik van medische gegevens door hulpverleners als dat noodzakelijk is voor de goede behandeling of verzorging van een betrokkene. In beginsel is geen van deze uitzonderingen van toepassing bij actieve openbaarmaking.

Identificatienummers vormen een aparte categorie bijzondere persoonsgegevens. Omdat persoonsnummers de koppeling van verschillende bestanden vergemakkelijken, vormen ze een extra bedreiging voor de persoonlijke levenssfeer. Volgens artikel 24 Wbp mogen wettelijk voorgeschreven nummers ter identificatie van personen alleen worden gebruikt voor de uitvoering van de betreffende wet of voor doeleinden die bij de wet zijn bepaald. Dit betekent in de praktijk dat het niet is toegestaan om bijvoorbeeld iemands BSN (burgerservicenummer) op internet te publiceren, zelfs niet als de betrokkene er toestemming voor heeft gegeven.

### 1.6.1 Uitzonderingen op het verbod om bijzondere persoonsgegevens te publiceren

Het verwerken van bijzondere persoonsgegevens is in beginsel niet toegestaan. Wie toch bijzondere persoonsgegevens openbaar wil maken, kan gebruik maken van een van de twee hierboven vermelde algemene uitzonderingen op het verwerkingsverbod, uitdrukkelijke toestemming van de betrokkene of het feit dat de gegevens door de betrokkene bewust zelf openbaar zijn gemaakt.

#### *Uitdrukkelijke toestemming*

Met het begrip 'uitdrukkelijke toestemming' stelt de Wbp een zware eis aan de kwaliteit van de toestemming. Die mag niet impliciet of stilzwijgend zijn; de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking.<sup>31</sup> De uitdrukkelijke individuele toestemming kan dus niet vervangen worden door het aanbieden van een mogelijkheid om de gegevens te laten verwijderen (ook wel een 'opt out' genoemd).

#### *Zelf openbaar gemaakt*

De situatie dat de betrokkene de gegevens zelf openbaar heeft gemaakt zal zich bij *structurele* actieve openbaarmaking niet voordoen. Wel is het denkbaar dat een bestuursorgaan in incidentele gevallen gegevens openbaar maakt die eerder ook door de betrokkene in de openbaarheid zijn gebracht. Niet voldoende is dat de gegevens al eerder door hetzelfde bestuursorgaan openbaar gemaakt zijn, bijvoorbeeld in reactie op een Wob-verzoek.

#### VOORLICHTING DOOR HET OM, VERDONK VS. PASIC

De uitzondering dat de betrokkene de gegevens zelf openbaar heeft gemaakt geldt alleen als de *specifieke* gegevens al in de openbaarheid zijn gebracht. Het is niet voldoende dat de betrokkene in een bepaalde zaak zelf ook de openbaarheid heeft gezocht. In dit verband schreef het CBP in zijn jaarverslag over 2006 het volgende over de nieuwe Aanwijzing Voorlichting, opsporing en vervolging van het Openbaar Ministerie:

"Het CBP acht de nieuwe aanwijzing grotendeels een verbetering. Over een belangrijk punt verschillen het CBP en het OM echter van mening. De Aanwijzing bepaalt dat wanneer verdachten of hun advocaat informatie over hun strafzaak openbaar maken het OM ervan uit gaat dat zij in redelijkheid geen bezwaar meer kunnen maken tegen de schending van hun privacy in die zaak.

Het CBP stelt zich op het standpunt dat als burgers of advocaten zich in de ogen van het OM misdragen door feiten – al dan niet op misleidende wijze – uit een strafdossier aan de openbaarheid prijs te geven, dat nog geen reden is om dat zelf ook te gaan doen. Het OM beschikt over bijzondere machtsmiddelen. Per geval zal de afweging moeten worden gemaakt of verstrekking van persoonsgegevens in re-

<sup>31</sup> MvT, blz. 122–123.

delijke verhouding staat tot het belang van de betrokkene en diens recht op bescherming van de persoonlijke levenssfeer. Voorkomen moet worden dat de verstrekte informatie direct of indirect kan leiden tot op individuele personen te herleiden informatie. De in individuele dossiers verzamelde gegevens zijn niet bedoeld om het OM te wapenen tegen onheuse aanvallen in media.

Het OM is bij de uitoefening van zijn taak gehouden het grondrecht op bescherming van de persoonlijke levenssfeer te respecteren. Als een verdachte zelf de publiciteit zoekt, wil dat niet zeggen dat hij daarmee zijn recht op grondrechtelijke bescherming verspeelt. Deze afweging is eerder in 2006 aan de orde geweest in het onderzoek dat het CBP heeft gedaan naar de verstrekking van persoonsgegevens van Taida Pasic aan de Telegraaf door minister Verdonk van Vreemdelingenzaken en Integratie. Het CBP concludeerde toen onder meer dat deze handelwijze van de minister een inbreuk maakte op de bescherming van de persoonlijke levenssfeer van Pasic die niet in verhouding stond tot het door de bewindsvrouw aangevoerde belang van informatieverstrekking. De verstrekking van – deels ook nog onjuiste en kwalificerende – persoonsgegevens was onverenigbaar met het doel waarvoor de gegevens waren verkregen, namelijk het nemen van een beslissing over de door Pasic gevraagde verblijfsvergunning.”

## 1.7 Internationaal kader

Deze richtsnoeren zijn gebaseerd op de Nederlandse wet- en regelgeving. Deze is echter ingebed in een Europees regelgevingskader. Daarvan zijn met name het Europees gegevensbeschermingsverdrag<sup>32</sup> (waarbij Nederland partij is<sup>33</sup>) en de Europese gegevensbeschermingsrichtlijn 95/46/EU in dit kader relevant. Richtlijn 95/46 is door de Artikel 29-werkgroep uitgewerkt voor actieve openbaarmaking in zijn *Advies 3/99 betreffende Overheidsinformatie en de bescherming van persoonsgegevens* (WP20). Dit advies is daarmee dé referentie voor het Europese kader ten aanzien van de bescherming van persoonsgegevens bij actieve openbaarmaking. Een heldere analyse van de Raad van Europa, met als vertrekpunt het Europees gegevensbeschermingsverdrag, is te vinden in *Recommendation No. R (91) 10 of the Committee of Ministers to Member States on the Communication of third parties of personal data held by public bodies*. De belangrijkste aanbevelingen uit beide genoemde documenten zijn opgenomen in de bijlage.

---

<sup>32</sup> Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg, 28 januari 1981, Trb. 1988, 7.

<sup>33</sup> Goedkeuringswet Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Staatsblad 1991, 654.

## 2 Verplichtingen van de verantwoordelijke

### 2.1 Inleiding

Onrechtmatig openbaar gemaakte persoonsgegevens moeten door de verantwoordelijke onmiddellijk van internet worden verwijderd. Maar ook voorafgaand aan het actief openbaar maken van persoonsgegevens dient het verantwoordelijke bestuursorgaan een aantal stappen te doorlopen om onrechtmatigheid te voorkomen. Dit hoofdstuk van de richtsnoeren bevat aanwijzingen voor de verantwoordelijke om in de fasen voorafgaand aan, tijdens en volgend op publicatie aan de vereisten van de Wet bescherming persoonsgegevens te voldoen.

Zoals in het onderstaande zal worden uitgelegd dient de verantwoordelijke voorafgaand aan de openbaarmaking vast te stellen of deze een legitiem doeleinde dient en of dat doel verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verkregen. De verantwoordelijke dient te kunnen onderbouwen dat de openbaarmaking wettelijk verplicht is of noodzakelijk voor de goede vervulling van een publiekrechtelijke taak die hem als bestuursorgaan is opgedragen. Eventueel kan de betrokkenen ook om toestemming worden gevraagd.

Bij openbaarmaking dienen verantwoordelijken betrokkenen actief te informeren over het doel en de opzet daarvan. Daarnaast moet iedere verantwoordelijke zijn eigen identiteit duidelijk vermelden, toegankelijk voor iedere bezoeker van de publicatie.

Persoonsgegevens mogen niet langer bewaard en ter beschikking worden gesteld dan strikt noodzakelijk. Bovendien moet de verantwoordelijke actief de kwaliteit en juistheid van actief openbaar gemaakte persoonsgegevens waarborgen.

Een laatste belangrijke stap die verantwoordelijken moeten nemen om te voldoen aan de vereisten van de Wbp is het treffen van beveiligingsmaatregelen tegen onbevoegd gebruik.

Ten slotte dienen verantwoordelijken zich bewust te zijn van de verplichting om ook na de openbaarmaking nog wijzigingen aan te brengen, bijvoorbeeld als een betrokkene zijn toestemming voor openbaarmaking intrekt, als de betrokkene terecht verzet aantekent op basis van zijn bijzondere persoonlijke omstandigheden of als de actieve openbaarmaking van de gegevens onrechtmatig blijkt te zijn.

Het is voor verantwoordelijken van belang om zich te realiseren dat het hier niet om een aantal los van elkaar staande elementen gaat. De diverse randvoorwaarden kunnen elkaar onderling beïnvloeden. Zo zal er sneller sprake zijn van verenigbaar gebruik naarmate betrokkenen beter geïnformeerd zijn, zij op eenvoudiger wijze hun rechten kunnen uitoefenen en de gegevens beter beveiligd zijn tegen onrechtmatig verder gebruik.

#### *Doorgifte buiten de EU*

Het doorgeven van persoonsgegevens naar landen buiten de EU is verboden, tenzij een van de wettelijke uitzonderingen van toepassing is. Hoewel actief openbaar gemaakte gegevens doorgaans ook toegankelijk zijn in landen buiten de EU, wordt deze toegankelijkheid niet als doorgifte beschouwd. Om de extra risico's van toegankelijkheid in landen buiten de EU te ondervangen, hebben verantwoordelijken voor via internet openbaar gemaakte gegevens wel meer nog dan andere verantwoordelijken de plicht om behoorlijk en zorgvuldig te werk te gaan en betrokkenen goed te informeren over de specifieke risico's van beschikbaarheid van de gegevens buiten de EU. Zie voor meer hierover hoofdstuk V van de CBP Richtsnoeren voor publicatie van persoonsgegevens op internet.

#### ➤ VOORAFGAAND AAN PUBLICATIE

### 2.2 Legitieme doeleinden

Wie persoonsgegevens van derden wil publiceren op internet, moet zich afvragen of hij de gegevens verzamelt en gebruikt voor een legitiem doeleinde. Artikel 7 van de Wbp

legt vast dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. Een voorbeeld van zo'n doeleinde is het in staat stellen van (derden) belanghebbenden om bezwaar te maken tegen een voorgenomen beschikking of daar juist van af te zien. Een doeleinde mag niet zo ruim of vaag zijn dat zij geen kader biedt om te toetsen of de gegevens noodzakelijk zijn voor het gestelde doel.

#### Belangenafweging noodzakelijk

Bestuursorganen die het noodzakelijk achten om in het kader van een publieksvriendelijke uitoefening van hun publiekrechtelijke taken persoonsgegevens op internet te publiceren, dienen een gedegen proportionaliteitsafweging te maken, allereerst voor de publicatie als geheel, en vervolgens voor elk soort gegeven dat zij op internet menen te moeten publiceren, variërend van achternaam en adres tot kwalitatieve beoordelingen en bijzondere persoonsgegevens met betrekking op bijvoorbeeld iemands gezondheid of politieke voorkeur. Bezien moet worden of de risico's voor betrokkenen niet zwaarder moeten wegen dan het belang van het bestuursorgaan bij publicatie van ieder specifiek soort gegeven. Daarbij dient de verantwoordelijke rekening te houden met de bijzondere risico's van openbaarmaking op internet. Inherent aan publicatie op internet is immers dat onbekende derden de gegevens op schadelijke wijze kunnen gebruiken, bijvoorbeeld voor het plegen van identiteitsfraude. Ook dienen verantwoordelijken het cumulatief effect mee te laten wegen van het geheel aan persoonsgegevens dat zij over personen op internet publiceren, en zelfs – voor zover zij dat redelijkerwijs kunnen inschatten – het cumulatieve effect van combinatie van de door hen gepubliceerde gegevens met andere gegevens die over dezelfde betrokkenen op het internet te vinden zijn.

Iedere vorm van openbaarmaking brengt zijn eigen risico's met zich mee. Dat betekent dat het feit dat een bepaald gegeven al eerder door het bestuursorgaan openbaar is gemaakt (bijvoorbeeld in reactie op een Wob-verzoek) in het algemeen niet als argument ten faveure van openbaarmaking kan gelden. Welke persoonsgegevens precies openbaar gemaakt kunnen worden hangt dus samen met de vorm van openbaarmaking. Het gebruik van gemarkeerde tekst<sup>34</sup> kan behulpzaam zijn bij het tot stand brengen van deze differentiatie.

### 2.3 Verdere verwerking

Bij het publiceren op internet van gegevens die voor een ander doeleinde zijn verzameld, dient de verantwoordelijke vast te stellen of publicatie op internet verenigbaar is met die doeleinden. Artikel 9 van de Wbp stelt een afweging verplicht tussen het oorspronkelijke doeleinde en de verdere verwerking en geeft daarbij vijf criteria waarmee in elk geval rekening moet worden gehouden:

- a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- b. de aard van de betreffende gegevens;
- c. de gevolgen van de beoogde verwerking voor de betrokkene;
- d. de wijze waarop de gegevens zijn verkregen;
- e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Het feit dat een bestuursorgaan over persoonsgegevens beschikt, betekent dus niet dat ze zomaar actief openbaar gemaakt mogen worden, voor een ander doeleinde dan waarvoor ze zijn verkregen. Het nieuwe doel moet verenigbaar zijn met het oude doel en de verantwoordelijke dient een zelfstandige rechtvaardigingsgrond te hebben voor de publicatie (zie paragraaf 2.5 hieronder: toestemming vragen of noodzaak kunnen aantonen).

Een verantwoordelijke kan zich omgekeerd ook de vraag stellen welke maatregelen hij kan treffen om te bewerkstelligen dat een voorgenomen actieve openbaarmaking verenigbaar is met het doel waarvoor de betreffende gegevens zijn verkregen. Vaak zal de

---

<sup>34</sup> Bijvoorbeeld gebaseerd op het snel aan populariteit winnende XML-formaat.

wijze van actieve openbaarmaking hierbij de sleutel vormen. Gelet op de risico's voor betrokkenen zal actieve openbaarmaking door bijvoorbeeld ter inzage legging in het algemeen veel sneller verenigbaar zijn dan publicatie van de persoonsgegevens op internet. Andere voorbeelden van mogelijke maatregelen zijn het beperken van toegang tot de gegevens, het beperken van de set te publiceren gegevens, het vooraf goed informeren van de betrokken burgers en het creëren van een eenvoudige mogelijkheid voor de betrokkene om verzet tegen de openbaarmaking aan te tekenen.

Ook de aard van de betreffende gegevens kan bij het beoordelen van de verenigbaarheid een gewichtige rol spelen. Zo wordt gedetailleerde informatie over inkomen en vermogen algemeen aangemerkt als privacygevoelig en zal het openbaar maken ervan daarom niet snel verenigbaar zijn met het oorspronkelijke verzameldoel (bijv. belastinginning).

Om onverenigbaarheid te voorkomen van de publicatie van persoonsgegevens op internet, dient het bestuurorgaan ten slotte nog zorgvuldig af te wegen of de risico's voor sommige groepen betrokkenen niet te groot zijn. Het bestuursorgaan hoeft met andere woorden niet voor iedere betrokkene een individuele afweging te maken.<sup>35</sup> Het dient echter wel een redelijke inspanning te leveren om na te gaan of er zich in de groep van personen waarover gegevens openbaar gemaakt worden geen subgroepen bevinden waarvoor de belangenafweging anders uitvalt dan in het algemene geval.

#### NIET ALLE AANVRAGEN VAN BOUWVERGUNNINGEN OP INTERNET

De gemeente Nijmegen publiceert bepaalde gegevens over lopende aanvragen voor bouwvergunningen op internet, teneinde (derden) belanghebbenden in staat te stellen om op eenvoudige wijze kennis te nemen van een voorgenomen beschikking en daar desgewenst bezwaar tegen te maken. Met het oog op de bijzondere risico's worden echter geen gegevens gepubliceerd van aanvragen voor vergunningen voor bouwwerken met een verhoogd risico voor de openbare veiligheid zoals banken, tbs-klinieken, gevangenissen, geldautomaten, ambassades en Blijf-van-mijn-lijfhuizen.

Het verenigbaarheidsvereiste uit de Wbp heeft sterke raakvlakken met bepalingen in de wet over de kwaliteit en beveiliging van gegevens. Zelfs als het nieuwe doel verenigbaar is met het oude doel, kan de verwerking onrechtmatig zijn, bijvoorbeeld als het gaat om het openbaar maken van verouderde of anderszins onjuiste informatie. De onderwerpen kwaliteit en beveiliging komen nader aan de orde in de paragrafen 2.7 en 2.8 van dit hoofdstuk. Daarnaast geldt het algemene uitgangspunt (uit artikel 6 Wbp) dat verantwoordelijken op behoorlijke en zorgvuldige wijze te werk dienen te gaan bij het verzamelen en verwerken van persoonsgegevens. Deze bepaling speelt zeker bij de beoordeling van de verenigbaarheid van publicaties op internet een belangrijke rol.

### 2.3.1 Verder gebruik van persoonsgegevens

Verantwoordelijken dienen zich bij het beoordelen of actieve openbaarmaking van persoonsgegevens verenigbaar is met het oorspronkelijke doeleinde niet alleen rekenschap te geven van het doeleinde waarvoor de gegevens zijn verzameld, maar ook van het risico dat anderen de gegevens voor andere doeleinden gebruiken dan waarvoor ze openbaar gemaakt worden. Om de risico's voor betrokkenen te verkleinen, dient elke verantwoordelijke adequate beveiligingsmaatregelen te treffen tegen oneigenlijk verder gebruik.

Voor een juiste risico-inschatting is het essentieel dat de rol van zoekmachines wordt meegewogen. Publicaties op internet die eigenlijk gericht zijn op een klein publiek, worden door zoekmachines wereldwijd toegankelijk gemaakt. Zoekmachines kunnen de aandacht vestigen op onvermoede gegevens over een persoon en daarnaast verspreide informatie van verschillende aard over een persoon koppelen. Dat kan een nieuw beeld

<sup>35</sup> Tenzij de betrokkene gebruik maakt van zijn bijzondere recht op verzet, zie § 3.4.

opleveren, met een veel hoger risico voor de betrokkene dan elk van de afzonderlijke gegevens meebrengt. Daarnaast bestaat er een reëel risico van persoonsverwisseling, waardoor verkeerde gegevens op een persoon betrokken kunnen worden. Strikte inperking van de gebruiksmogelijkheden en afscherming van persoonsgegevens voor zoekmachines zijn daarom belangrijke maatregelen om oneigenlijk hergebruik te voorkomen. Dit vereiste wordt nader uitgewerkt in paragraaf 2.8.3 van dit hoofdstuk.

### 2.3.2 Geheimhoudingsplicht

De Wbp verbiedt publicatie van persoonsgegevens indien de gegevens onder een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift vallen.<sup>36</sup> Deze bepaling wordt dikwijls ingezet in zaken waarin het medisch beroepsgeheim speelt, maar is door het CBP ook gehanteerd bij het beoordelen van een overheidsinitiatief om persoonsgegevens openbaar te maken via internet.

#### PUBLICATIE WAARDEGEGEVENS ONROEREND GOED

In 2003 vroeg het Ministerie van Financiën advies aan het CBP over een aantal voorgenomen wijzigingen in de Wet waardering onroerende zaken (Wet WOZ). Het voorstel beoogde de openbaarheid van WOZ-gegevens te vergroten door de taxatierapporten op internet te plaatsen. Het CBP adviseerde<sup>37</sup>: 'Gelet op het vorenstaande komt het CBP tot het oordeel dat een algemene toegankelijkheid van waardegegevens op het internet zich niet verhoudt met de Wbp en de Wet WOZ. Het CBP onderschrijft het oordeel van de Raad van State dat het waardegegeven privacygevoelige informatie betreft. Verdere verwerking van deze gegevens (door plaatsing op het internet) dient daarom op grond van het bepaalde in artikel 40, eerste lid, Wet WOZ en artikel 9, vierde lid, Wbp achterwege te blijven.'

## 2.4 Toestemming vragen of noodzaak kunnen aantonen

Voor verantwoordelijken die persoonsgegevens openbaar willen maken, geldt dat zij toestemming nodig hebben van de betrokkenen, of dat er een aantoonbare noodzaak moet zijn voor de openbaarmaking, zoals nakoming van een wettelijke verplichting. Op dit punt schept de Wbp dus niet alleen waarborgen: zonder een rechtvaardigingsgrond in de Wbp is het verwerken van persoonsgegevens niet toegestaan.

### 2.4.1 Toestemming

Toestemming moet ondubbelzinnig zijn (in het geval van bijzondere persoonsgegevens zelfs 'uitdrukkelijk'). De verantwoordelijke mag niet uitgaan van het principe 'wie zwijgt, stemt toe', maar moet elke twijfel uitsluiten over de vraag of de betrokkene toestemming heeft gegeven, en zo ja, voor welke specifieke verwerkingen die geldt. Een eenmaal gegeven toestemming kan te allen tijde worden ingetrokken.<sup>38</sup> Het bestuursorgaan dient een adequate procedure in te richten om aan dergelijke verzoeken te kunnen voldoen.

Toestemming speelt in de praktijk vooral een rol als rechtvaardigingsgrond bij het publiceren van aanvullende gegevens. Denk bijvoorbeeld aan het bij vergunningsaanvragen publiceren van contactinformatie van de aanvrager die derden graag de mogelijkheid geeft om daarover rechtstreeks met hem in contact te treden. Vanwege de mogelijkheid tot het intrekken ervan zal toestemming echter slechts zelden op zichzelf een werkbare rechtvaardigingsgrond zijn voor actieve openbaarmaking, ook omdat de openbaarmaking dan al snel in strijd komt met andere uitgangspunten, zoals het niet meer gegevens ver-

<sup>36</sup> Wbp, artikel 9, lid 4.

<sup>37</sup> CBP, z2003-01563, 11 februari 2004, URL: [http://www.cbpweb.nl/documenten/adv\\_z2003-1563.stm](http://www.cbpweb.nl/documenten/adv_z2003-1563.stm)

<sup>38</sup> Artikel 5 Wbp tweede lid: 'Een toestemming kan door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.'

werken dan noodzakelijk is met het oog op de doeleinden van de verwerking.<sup>39</sup> We gaan er daarom hier niet verder op in.<sup>40</sup>

#### CWI PUBLICEERT GEGEVENS WERKZOEKENDEN OP INTERNET

Naar aanleiding van berichten in de media dat privégegevens van werkzoekenden vrij toegankelijk waren via de vacaturesite werk.nl heeft het CBP het Centrum voor werk en inkomen in april 2004 om opheldering gevraagd. Uit de verstrekte informatie bleek dat werkzoekenden zelf konden besluiten of zij naast gegevens over opleiding en werkervaring ook andere persoonsgegevens (zoals naam, adresgegevens en telefoonnummer) op internet wilden plaatsen. Het privacystatement van het CWI vermeldde duidelijk dat deze gegevens openbaar toegankelijk waren voor anderen. Het CWI heeft inmiddels wel restricties aangebracht in deze toegang tot gegevens van werkzoekenden. Alleen werkgevers met een zogenaamd werkgeversaccount kunnen nu direct alle gegevens van werkzoekenden opvragen.<sup>41</sup>

### 2.4.2 Noodzaak

De Wbp kent vijf rechtvaardigingsgronden die gebaseerd zijn op een aantoonbare noodzaak voor de verantwoordelijke. Dat zijn: uitvoering van een overeenkomst, voldoen aan een specifieke wettelijke verplichting, vitaal belang, een goede vervulling van een specifieke publiekrechtelijke taak of een afweging van belangen.

Uitvoering van een overeenkomst en het vitaal belang van de betrokkene zijn onwaarschijnlijke rechtvaardigingsgronden voor actieve openbaarmaking. Hieronder komen daarom slechts de drie andere rechtvaardigingsgronden aan de orde. Zoals in de betreffende paragraaf nader zal worden toegelicht zal een afweging van belangen overigens ook zelden een rechtvaardigingsgrond vormen voor actieve openbaarmaking.

#### 2.4.2.1 Goede vervulling van een publiekrechtelijke taak

In de volgende paragraaf zal nader uiteengezet worden dat in het licht van de Wbp andere wetten, waaronder de Wob, slechts zeer beperkte mogelijkheden bieden tot het actief openbaar maken van persoonsgegevens. Bestuursorganen beschikken wel over een andere rechtvaardigingsgrond in de Wbp die het in bepaalde gevallen mogelijk maakt over te gaan tot actieve openbaarmaking van persoonsgegevens. Artikel 8 onder e Wbp bepaalt dat een rechtvaardigingsgrond voor de verwerking van persoonsgegevens is dat deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan.<sup>42</sup> In de Memorie van Toelichting bij de Wbp is dit criterium als volgt toegelicht (blz. 84):

Het gaat in onderdeel e om een gegevensverwerking in het belang van een publiekrechtelijke taak die wordt uitgeoefend door het desbetreffende bestuursorgaan (...). De gegevensverwerking moet wel noodzakelijk zijn voor de vervulling van de betrokken taak van het bestuursorgaan. Als er geen gedetailleerde wettelijke regels bestaan voor deze taakuitoefening, dient bijzondere aandacht te worden besteed aan de vraag of wel sprake is van een rechtmatige taakuitoefening. Om deze reden spreekt onderdeel e ook van een 'goede vervulling' van de taak. Bij de beoordeling van de noodzaak van de betrokken verwerking zullen verder de beginselen van proportionaliteit en subsidiariteit een belangrijke rol spelen.

<sup>39</sup> Artt. 10 en 11 Wbp.

<sup>40</sup> Zie voor meer informatie de CBP Richtsnoeren voor publicatie van persoonsgegevens op internet.

<sup>41</sup> CBP, april 2004, z2003-1437, URL: [http://www.cbpweb.nl/documenten/uit\\_z2003-1437.stm](http://www.cbpweb.nl/documenten/uit_z2003-1437.stm)

<sup>42</sup> Het andere deel van dit lid, noodzakelijk voor de goede vervulling van het bestuursorgaan waaraan de gegevens worden verstrekt, is hier niet aan de orde aangezien het bij actieve openbaarmaking gaat om een algemene, ongerichte verstrekking.

Artikel 8 onder e Wbp biedt met andere woorden een rechtvaardigingsgrond voor actieve openbaarmaking van persoonsgegevens indien:

- deze openbaarmaking van belang is voor de goede vervulling van een specifieke publiekrechtelijke taak van het betreffende bestuursorgaan;
- dat belang onvoldoende gediend kan worden door minder ingrijpende maatregelen, zoals passieve openbaarmaking of openbaarmaking via ter inzage legging;
- dat belang zwaarder weegt dan het belang van de betrokkenen bij de bescherming van hun persoonsgegevens.

#### VERGUNNINGEN OP INTERNET

Onder auspiciën van BZK plaatsen veel gemeenten en bestuursorganen informatie over bestuurlijke aangelegenheden op internet. Ten minste één gemeente heeft in dat kader zijn volledige bestand van aangevraagde en verleende bouwvergunningen, inclusief onderliggende stukken, op internet geplaatst.

Het CBP oordeelde hierover als volgt:

“De gemeente heeft niet kunnen onderbouwen dat het integraal publiceren van de documenten met persoonsgegevens op internet noodzakelijk zou zijn voor een goede vervulling van de publiekrechtelijke taak door de gemeente (...). De gemeente kan zich daarom niet beroepen op een grondslag onder artikel 8 onder e Wbp.

Voor het kenbaar maken van zienswijzen of bezwaar maken tegen beschikkingen omtrent vergunningen, zoals bedoeld in de Awb is het niet noodzakelijk om te beschikken over alle persoonsgegevens van een aanvrager van een vergunning. Het omschrijven van het besluit waartegen het bezwaar of beroep is gericht, is voldoende, naast een inhoudelijke motivering van het bezwaar of beroep.

Het CBP stelt vast dat het noch voor de vergunningsaanvrager, noch voor (derden) belanghebbenden noodzakelijk is om voor het uitoefenen van hun rechten toegang te hebben tot de integraal ingescande aanvragen met een keur aan persoonsgegevens. De door de gemeente beoogde transparante gegevensverwerking wordt adequaat gediend met publicatie op internet van beperkte informatie over het proces van het aanvragen tot het verlenen of weigeren van vergunningen, namelijk het adres, een omschrijving van het soort vergunning en – mits de aanvrager daartegen geen steekhoudend bezwaar maakt op grond van bijzondere omstandigheden – de bijbehorende bouwtekeningen.

Een bijzonder geval in deze categorie is nog openbaarmaking op grond van meer algemene openbaarheidsregimes, die niet specifiek over *gegevens* gaan. Daarbij is met name te denken aan twee grondwettelijk verankerde openbaarheidsregimes:

- openbaarheid van rechtspraak (art. 121 Grondwet);
- openbaarheid van vergaderingen van het openbaar bestuur (o.a. art. 66 Grondwet).

Essentieel hierbij is dat de betreffende regelgeving alleen rept over de openbaarheid van de betreffende bijeenkomsten (terechtzingen en uitspraken resp. vergaderingen), niet over openbaarheid van informatie over die bijeenkomsten. Dit betekent dat er geen wettelijke verplichting bestaat tot het openbaar maken (laat staan het actief openbaar maken via internet) van zulke informatie. Indien de betrokken bestuursorganen niettemin tot actieve openbaarmaking willen overgaan en daarbij ook persoonsgegevens in het spel zijn, zullen zij zich moeten beroepen op de noodzaak voor de goede vervulling van de hun opgedragen publiekrechtelijke taken.<sup>43</sup>

<sup>43</sup> In een enkel geval kan ook een beroep mogelijk zijn op een ander gerechtvaardigd belang dat zij hebben, zie paragraaf 2.4.2.3.

In het kader bij deze paragraaf wordt dit uitgewerkt voor rechterlijke uitspraken. Zie ook het kader bij paragraaf 2.7.1 over gemeenteraadsvergaderingen.

#### RECHTSPRAAK.NL

Rond de eeuwwisseling zijn diverse rechterlijke instanties overgegaan tot het actief openbaar maken van uitspraken via internet. Het meest in het oog springende voorbeeld was de inrichting van de website [www.rechtspraak.nl](http://www.rechtspraak.nl). Via deze website wordt een belangrijk deel van de Nederlandse jurisprudentie voor het publiek ontsloten.

Tot op heden is bij elektronische verspreiding van rechterlijke uitspraken steeds het uitgangspunt geweest dat gegevens van natuurlijke personen zoveel mogelijk worden vervangen door neutrale termen als eiser, verweerder of een kwalificerende omschrijving, alvorens tot publicatie over te gaan. Geregeld vallen er echter pleidooien te lezen voor het niet-geanonimiseerd beschikbaar maken van rechterlijke uitspraken, al dan niet met uitzonderingen of mogelijkheden voor betrokkenen om bezwaar te maken.<sup>44</sup>

Burgers zijn bevreesd voor publiciteit over rechtszaken waarin zij – al dan niet door eigen toedoen – in betrokken raken. Het CBP ontvangt regelmatig klachten over perspublicaties over rechtszaken. Bij voortdrijving wordt aangedrongen op meer mogelijkheden om anoniem te getuigen. De rechterlijke macht heeft met de pers afspraken gemaakt over het zo min mogelijk publiceren van (voor)namen van individuele rechters in perspublicaties. De ontwikkeling van de informatiesamenleving wordt enerzijds als zeer positief ervaren, maar men voelt zich ook kwetsbaarder.

Indien er niet langer geanonimiseerd zou worden zouden de royale mogelijkheden en langdurige beschikbaarheid van de rechterlijke uitspraken [rechtspraak.nl](http://rechtspraak.nl) kunnen maken tot een gegevensverzameling over personen die de wijze waarop zij in het maatschappelijk verkeer behandeld worden op onaanvaardbare wijze nadelig beïnvloedt. Te denken valt aan het gebruik van [rechtspraak.nl](http://rechtspraak.nl) voor screeningsdoeleinden. Heeft deze sollicitant wel eens in een arbeidszaak geprocedeerd? [Rechtspraak.nl](http://rechtspraak.nl) zou een nieuwe vorm van documentatie over personen opleveren, die haaks staat op gemaakte keuzes voor de bestaande – al dan niet openbare – registers waarin rechterlijke uitspraken ten behoeve van verschillende screeningsdoeleinden zijn verwerkt.

Integrale openbaarmaking van uitspraken kan zo bovendien tot vraaguitval leiden bij de rechtzoekenden en de facto de toegang tot het recht verminderen.

Gelet hierop zou integrale openbaarmaking van (alle) rechterlijke uitspraken op [rechtspraak.nl](http://rechtspraak.nl) te ver gaan. De toegang tot rechterlijke uitspraken kan worden verbeterd. Het is daarvoor echter niet noodzakelijk om tot (blijvende) integrale publicatie van uitspraken over te gaan.

#### 2.4.2.2 Wettelijke verplichting

Het moeten nakomen van een wettelijke verplichting is een rechtvaardigingsgrond die naar verwachting in de toekomst steeds vaker door overheidsinstellingen of beheerders van openbare registers gebruikt kan worden voor actieve openbaarmaking, en in het bijzonder actieve openbaarmaking via internet. Er is veel wetgeving in ontwikkeling ter bevordering van de transparantie en eenvormigheid van de besluitvorming door bestuursorganen. Daarbij wordt elektronische publicatie van persoonsgegevens soms expliciet voorgeschreven.

<sup>44</sup> Zie bijvoorbeeld *Toegang tot rechterlijke uitspraken*. Rapport van de VMC-studiecommissie Openbaarheid van rechtspraak. Mediaforum 2006-4.

De nu geldende wetgeving bevat daarentegen slechts weinig mogelijkheden om het moeten nakomen van een wettelijke verplichting aan te voeren als rechtvaardigingsgrond voor actieve openbaarmaking, zeker actieve openbaarmaking op internet. Dat is het gevolg van een combinatie van factoren. In de eerste plaats dient de wet niet alleen de *mogelijkheid* maar een duidelijke *verplichting* tot openbaarmaking te scheppen. Ten tweede dient dat niet een algemene verplichting tot openbaarmaking te zijn, maar een specifieke verplichting tot *actieve* openbaarmaking. Bij actieve openbaarmaking door publicatie op internet komt daar ten slotte nog de voorwaarde bij dat de wetsgeschiedenis de conclusie wettigt dat de belangen van openbaarmaking ook zwaarder wegen dan de extra risico's die publicatie op internet met zich meebrengt. In alle andere gevallen zal een rechtvaardigingsgrond gevonden moeten worden in de noodzaak voor goede vervulling van een publiekrechtelijke taak.<sup>45</sup>

Hieronder volgt een beknopt overzicht van de mogelijkheden voor verantwoordelijken om zich te beroepen op een wettelijke verplichting als rechtvaardigingsgrond voor actieve openbaarmaking. Daartoe worden drie wettelijke kaders voor openbaarmaking van gegevens besproken. Een uitgebreidere analyse is te vinden in Bijlage 2.

Het eerste geval is openbaarmaking op grond van specifieke wetgeving die een uitputtend regime bevat voor de verwerking van persoonsgegevens en de toepasselijkheid van de Wbp expliciet uitsluit. Het gaat hier om een beperkt aantal wetten.<sup>46</sup> Omdat de specifieke wetgeving een *uitputtend* regime bevat voor de betreffende gegevensverwerkingen, dient de verantwoordelijke een expliciete verplichting tot actieve openbaarmaking op de door hem voorgenomen wijze in de betreffende wet te kunnen aanwijzen. Artikel 8 onder e Wbp of artikel 8 Wob komen niet als rechtvaardigingsgrond in aanmerking.

Het tweede geval is openbaarmaking op grond van specifieke wetgeving die een regeling op deelterreinen van de bescherming van persoonsgegevens bevat en waarbij de Wbp aanvullend van toepassing is. Het gaat hier om een veelheid aan wettelijke regelingen.<sup>47</sup> De eerste vraag die de verantwoordelijke zich dient te stellen is of de betreffende wet een regeling bevat op het deelterrein van de gegevensverstrekking. Is dat zo, dan is de tweede vraag die de verantwoordelijke zich dient te stellen of deze regeling een duidelijke verplichting tot actieve openbaarmaking bevat. Alleen in dat geval kan hij de betreffende wet aanvoeren als rechtvaardigingsgrond voor actieve openbaarmaking. Bij actieve openbaarmaking door publicatie op internet komt daar ten slotte nog de eis bij van *internet als voorgeschreven medium* voor actieve openbaarmaking, óók als het gaat om bij wet ingestelde openbare registers.

Het derde en laatste geval is openbaarmaking op grond van generieke wetgeving voor de verwerking van gegevens, te weten de Wob. Voor deze wet zijn de drie vragen die de verantwoordelijke zich moet stellen in algemene zin te beantwoorden. De Wob bevat een duidelijke – voorwaardelijke<sup>48</sup> – verplichting tot *passieve* openbaarmaking (Hoofdstuk III Wob). Ten aanzien van *actieve* openbaarmaking is slechts sprake van een instructienorm tot beleidsvoorlichting. Deze kan in het algemeen niet worden gezien als wettelijke verplichting tot *actieve* openbaarmaking, laat staan tot actieve openbaarmaking *op internet*.

#### 2.4.2.3 *Gerechtvaardigd belang*

Artikel 8 onder f Wbp bepaalt dat verantwoordelijken een gegevensverwerking mogen doen indien dat noodzakelijk is voor de behartiging van het gerechtvaardigde belang van

---

<sup>45</sup> Zie daarvoor de vorige paragraaf.

<sup>46</sup> Te weten de Wet op de inlichtingen- en veiligheidsdiensten 2002, de Wet veiligheidsonderzoeken, de Wet politiegegevens, de Wet gemeentelijke basisadministratie persoonsgegevens, de Wet justitiële en strafvorderlijke gegevens en de Kieswet.

<sup>47</sup> Zie bijlage 2 voor een aantal voorbeelden.

<sup>48</sup> De uitzonderingsgronden en beperkingen van Hoofdstuk V Wob moeten niet van toepassing zijn. Voor persoonsgegevens houden die specifiek in: bijzondere persoonsgegevens niet openbaar maken, en andere persoonsgegevens slechts na een in het voordeel van openbaarheid uitgevallen belangenafweging.

de verantwoordelijke of een derde aan wie de gegevens worden verstrekt, "tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert." Deze rechtvaardigingsgrond is vooral van belang voor verantwoordelijken in de private sector. Bestuursorganen kunnen er minder gemakkelijk een beroep op doen, aangezien bij een belangenafweging onder artikel 8 onder f Wbp door de publieke sector zwaarder gemotiveerd moet worden dan bij een vergelijkbare belangenafweging door de private sector. De MvT bij de Wbp licht dit als volgt toe: *"Binnen de publieke sector geldt immers de rechtstreeks werkende grondwetsbepaling die de persoonlijke levenssfeer beschermt, mede tegen de achtergrond van de daarmee corresponderende verdragsbepalingen. Ook in gevallen dat het onderdeel zou leiden tot een inbreuk op de persoonlijke levenssfeer, en de bepaling in dat geval als een legitimerende grondslag zou moeten worden aangemerkt als bedoeld in artikel 10, eerste lid, van de Grondwet, dan nog mag in het licht van artikel 8 EVRM, deze inbreuk niet verdergaan dan noodzakelijk is."*

## ➤ BIJ PUBLICATIE

### 2.5 Informatieplicht

De Wbp bevat een informatieplicht. Verantwoordelijken voor actieve openbaarmaking moeten op eigen initiatief inzicht geven in het doel van de openbaarmaking, welke persoonsgegevens ze verwerken, hoe ze dat doen en wat hun identiteit is. Dat is geen eenmalige verplichting, maar geldt jegens elke persoon over wie zij gegevens verwerken.

De informatieplicht geldt als verantwoordelijken de gegevens rechtstreeks van de betrokkene verkrijgen (artikel 33 Wbp), maar ook als zij de gegevens op een andere manier verkrijgen, bijvoorbeeld door koppeling met bestanden van andere bestuursorganen (artikel 34 Wbp). Als er weinig risico's gemoeid zijn met de openbaarmaking en als betrokkenen redelijkerwijs weten in welke context bepaalde persoonsgegevens over hen op internet worden gepubliceerd, kan een verantwoordelijke volstaan met het verstrekken van passieve informatie over zijn identiteit en het doeleinde van de publicatie, bijvoorbeeld in de vorm van een privacyverklaring. In alle andere gevallen dient een verantwoordelijke alle betrokkenen op voorhand te informeren, met zoveel aanvullende informatie als nodig is om er zeker van te zijn dat betrokkenen begrijpen wat de bedoeling is en hoe zij zich eventueel tegen publicatie kunnen verzetten.

#### 2.5.1 Omvang informatieplicht

Hoe verantwoordelijken precies aan de informatieplicht uit de Wbp kunnen voldoen, is afhankelijk van een aantal factoren. De memorie van toelichting bij de Wbp geeft aan dat verantwoordelijken zoveel informatie moeten verstrekken als nodig is om in elk concreet geval een behoorlijke en zorgvuldige gegevensverwerking te waarborgen, of zij de gegevens nu zelf van de betrokkene krijgen, of indirect.<sup>49</sup> Dat betekent dat de omvang van de informatieplicht afhangt van de aard van de verantwoordelijke, de risico's die met de publicatie zijn gemoeid en de manier waarop de persoonsgegevens zijn verkregen. Wie met toestemming van de betrokkenen persoonsgegevens op internet publiceert en de persoonsgegevens heeft afgeschermd tegen verder gebruik door zoekmachines, kan volstaan met een beknopte vermelding van zijn identiteit en het doeleinde van de publicatie, voorafgaand aan de publicatie. Wie echter op grond van een andere rechtvaardigingsgrond, zoals een goede vervulling van zijn publiekrechtelijke taak, gegevens op internet wil publiceren, dient de betrokkenen veel uitgebreider, individueel te informeren en hen te wijzen op hun recht op verzet, zeker als niet op voorhand duidelijk is dat de gegevens ook op internet worden gepubliceerd. Alleen als de verantwoordelijke aannemelijk kan maken dat het individueel informeren een onevenredige inspanning vergt – waaronder wordt verstaan dat het informeren substantiële kosten meebrengt, een buitengewone inspanning kost bij het achterhalen van betrokkenen of stuit op technische onmogelijk-

---

<sup>49</sup> MvT, blz. 149–150.

heden – en er geen andere wegen openstaan om de betrokkenen via algemenere kanalen te informeren, vervalt de actieve informatieplicht. De verantwoordelijke moet in dat geval wel zorgvuldig vastleggen van wie en op welke wijze hij de gegevens heeft verkregen.

Een bestuursorgaan dat publicatie op internet overweegt, zal alle betrokkenen doorgaans dus zorgvuldig dienen te informeren over het welbepaalde doeleinde van de publicatie op internet en de risico's van publicatie op internet. Het bestuursorgaan dient betrokkenen bovendien in staat te stellen om hun rechten op verwijdering of verzet effectief uit te oefenen. De informatie dient verstrekt te worden op het moment van het verzamelen van de informatie, niet naderhand.

De informatieplicht heeft betrekking op verwerkingen die rechtmatig zijn. Het ontbreken van een gerechtvaardigd doeleinde en grondslag voor de verwerking kan niet gecompenseerd worden door te voldoen aan de informatieplicht.

In het geval van een aanvraag voor een vergunning zou het voor de betrokkene al bij het invullen van het formulier glashelder moeten zijn dat er bepaalde gegevens op internet worden gepubliceerd. Het bestuursorgaan kan niet volstaan met het sturen van een brief naderhand waarin melding wordt gemaakt van het feit dat het hele document ook op internet wordt of is gepubliceerd.

Blijkens de MvT bij de Wbp (blz. 149) is het onvoldoende informeren van de betrokkene niet slechts in strijd met artikel 33 en/of 34 Wbp, maar leidt het zelfs tot onrechtmatigheid van de verwerking, i.c. de openbaarmaking: *“De omstandigheid dat de onderhavige regeling een uitwerking vormt van het beginsel dat in artikel 6 is neergelegd heeft tot gevolg, dat overtredingen van de informatieplicht zullen leiden tot onrechtmatige verwerkingen.”*

### **2.5.2 Privacyverklaring**

Wie op basis van toestemming persoonsgegevens openbaar maakt, hoeft de betrokkenen (na het verkrijgen van de toestemming) niet afzonderlijk meer te informeren over zijn identiteit en doeleinden van de verwerking. Een goede invulling van de beknopte informatieplicht is dan het publiceren van een privacyverklaring. De CBP Richtsnoeren voor publicatie van persoonsgegevens op internet bevatten in paragraaf 5.3 een overzicht van de elementen die zo'n verklaring moet bevatten, en in de bijlage een model privacyverklaring.

### **2.5.3 Identiteitsvermelding**

De Wbp eist in het tweede lid van de artikelen 33 en 34 Wbp dat verantwoordelijken hun identiteit bekend moeten maken. Dat stelt betrokkenen in staat om hun rechten effectief uit te oefenen en rechtstreeks met verantwoordelijken in contact te treden. De aanbeveling van de Artikel 29-werkgroep uit 2001 over het online verzamelen van gegevens benadrukt dat bij de identiteit zowel het elektronische als het fysieke adres moet worden vermeld.

## **2.6 Meldingsplicht**

Verantwoordelijken zijn in beginsel verplicht om alle gegevensverwerkingen te melden bij het CBP, tenzij ze onder het Vrijstellingsbesluit vallen of een eigen functionaris voor de gegevensbescherming (FG) aanstellen.<sup>50</sup> Een melding bij het CBP betreft een beschrijving van een of meerdere gegevensverwerkingen. Artikel 27 eerste lid Wbp verplicht tot aanmelding van een voorgenomen verwerking, dat wil zeggen dat de melding dient te geschieden alvorens tot de verwerking wordt overgegaan. Omdat 'verwerking' ook betrek-

---

<sup>50</sup> Zie voor een algemene toelichting op de meldingsplicht het informatieblad 'Melden en vrijstellingen' voor verantwoordelijken, beschikbaar via de website van het CBP, URL: <http://www.cbpweb.nl>, onder 'nieuws en publicaties', 'publicaties', 'informatiebladen'.

king heeft op het verzamelen, houdt dit in dat de verantwoordelijke de verwerking moet melden voordat hij de beschikking krijgt over persoonsgegevens.<sup>51</sup>

De meldingen worden opgenomen in een openbaar register, dat kosteloos toegankelijk is via de website van het CBP, conform artikel 30 Wbp. Het feit dat een melding is opgenomen in het openbare register, betekent niet dat het CBP de verwerking heeft goedgekeurd of rechtmatig acht. De melding biedt dan ook geen garantie dat de verantwoordelijke in overeenstemming met de Wbp persoonsgegevens verwerkt.

De meldingsplicht uit de Wbp (en de onderliggende Europese privacyrichtlijn) dateert van voor de opkomst van actieve openbaarmaking en andere internetpublicatievormen. Het valt te betwijfelen of de wetgever de meldingsplicht heeft bedoeld voor de praktijk van gegevensverwerking op internet in de huidige vorm en omvang. Op dit moment gelden nog geen specifieke vrijstellingen voor internetpublicaties, al zijn er wel enkele in de maak. Die uitzonderingen zullen echter niet van toepassing zijn bij actieve openbaarmaking.<sup>52</sup>

Gegeven deze omstandigheden legt het CBP thans behoudens bijzondere omstandigheden alleen prioriteit bij het controleren van melding van publicaties die bijzondere persoonsgegevens bevatten (zie hoofdstuk I, paragraaf 8) en van publicaties die vanuit beveiligingsoogpunt grote risico's voor betrokkenen meebrengen, zoals het risico op identiteitsfraude.

## 2.7 Kwaliteit

De Wbp stelt eisen aan de bewaartermijn en kwaliteit van persoonsgegevens. Gegevens mogen niet langer verwijzen naar identificeerbare personen dan strikt noodzakelijk en de gegevens moeten juist zijn en ter zake dienend.

### 2.7.1 Beperkt bewaren

Bestuursorganen dienen zich rekenschap te geven van de tijdsbeperkingen die artikel 10 Wbp stelt aan de verwerking van persoonsgegevens. Het bestuursorgaan dient onderscheid te maken tussen de bewaartermijn van een papieren archief en de termijn van digitale beschikbaarstelling van documenten op internet. Artikel 10 tweede lid Wbp stelt dat een langere bewaartermijn (dan noodzakelijk voor de verwerkelijking van de doeleinden waarvoor ze worden verzameld of vervolgens worden verwerkt) alleen is toegestaan "voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard en de verantwoordelijke de nodige voorzieningen heeft getroffen teneinde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt." Er is dus geen grondslag voor een oneindige bewaartermijn (terbeschikkingstelling op internet) van documenten met persoonsgegevens op grond van artikel 10 tweede lid Wbp. Een bestuursorgaan dat de documenten wel oneindig lang op internet wil publiceren, dient de toegang tot het online archief effectief af te schermen tot mensen die de gegevens raadplegen voor historische, statistische of wetenschappelijke doeleinden.

Zie over de termijn van openbaarmaking ook paragraaf 1.5.

#### HET PUBLICEREN VAN VERGADERVERSLAGEN

Een gemeente kan besluiten de verslagen van raads- en commissievergaderingen op internet te zetten. Zo kunnen burgers die niet in de gelegenheid zijn om de vergadering bij te wonen alsnog kennis nemen van wat er is besproken. De gemeente dient daarbij wel een termijn vast te stellen hoe lang de verslagen op internet blijven staan, althans in zodanige vorm dat ze persoonsgegevens bevatten. Het gaat

<sup>51</sup> MvT, blz. 137.

<sup>52</sup> De meldingsplicht geldt weliswaar niet voor openbare registers, maar daarvan is bij actieve openbaarmaking in het algemeen geen sprake.

daarbij met name om de inbreng van of beraadslagingen over individuele burgers. Het voor langere tijd publiceren van de inbreng van raadsleden en anderen in functie stuit in het algemeen niet op bezwaren.

Om burgers de gelegenheid te geven alsnog op eenvoudige wijze kennis te nemen van wat er tijdens een vergadering is besproken lijkt een termijn van enkele maanden voldoende. Het gebruik van een systeem voor webpublicatie dat het mogelijk maakt deze termijn automatisch in te stellen, is een eenvoudig voorbeeld van het gebruik van *Privacy Enhancing Technologies*. Het lijkt bovendien niet nodig dat de verslagen (in tegestelling tot bijvoorbeeld de agenda's of de besluitenlijsten) voor zoekmachines indexeerbaar gemaakt worden.

Na het verstrijken van de vastgestelde termijn dient de gemeente zich te beperken tot bijvoorbeeld het publiceren van besluitenlijsten. Uiteraard kan het verslag van de vergadering totdat het offline gearchiveerd wordt wel op verzoek aan burgers ter beschikking gesteld worden.

Voor audio- en video-registratie ligt het wat anders, aangezien dit een verwerking is die door de meeste mensen ervaren wordt als een grotere privacy inbreuk dan alleen het schriftelijk vastleggen van hun woorden of handelingen. Niettemin staat de Wbp er in het algemeen niet aan in de weg dat openbare vergaderingen op internet uitgezonden worden. In dat geval dient betrokkenen echter wel de mogelijkheid te worden geboden om vooraf (of ter plekke, bijvoorbeeld door het opsteken van een hand) te kennen te geven dat zij niet op beeld of geluid vastgelegd willen worden. De opnamen (dan wel de uitzending of vastlegging ervan) kunnen dan tijdelijk worden onderbroken. Eventueel kunnen audio- of video-opnamen een beperkte tijd via internet beschikbaar blijven. In het algemeen zal die termijn in ieder geval eindigen op het moment dat het verslag van de betreffende vergadering beschikbaar is.

### 2.7.2 Toereikend, ter zake dienend en niet bovenmatig

Conform artikel 11 Wbp moeten de op internet gepubliceerde gegevens ter zake dienend en niet bovenmatig zijn. Zelfs als een bestuursorgaan heeft vastgesteld dat publicatie van bepaalde persoonsgegevens op internet in beginsel gerechtvaardigd is en niet onverenigbaar met het doeleinde waarvoor de gegevens zijn verkregen, kan de publicatie van sommige gegevens bovenmatig zijn aan het doeleinde. Dat kan bijvoorbeeld het geval zijn bij begeleidende brieven aan het bestuursorgaan of voor individuele gegevens, zoals de elektronische contactgegevens en de 'natte' handtekening. Een gevolg hiervan is dat actieve openbaarmaking door middel van het op internet publiceren van ingescande documenten doorgaans geen optie is. De verantwoordelijke die op deze wijze wil werken dient daarmee al bij het opstellen en ontwerpen van de betreffende documenten en formulieren rekening te houden.

#### Toegang voor advocaten tot rolgegevens

Advocaten hebben belang bij toegang tot het rolregister van de rechtbank waar ze procederen. Toegang tot de gegevens van een rechtbank in een andere stad loopt voor advocaten via een vertegenwoordiging, een zogenaamde procureur. Het rolregister bevat informatie over alle aanhangige civiele zaken, met een korte typering, de namen van de eiser en de gedaagde, de namen van de procureurs en de status van de behandeling. In 2002 besloot de Raad voor de Rechtspraak tot invoering van een digitale rol, 'Mijn Zaken', waarbij advocaten via internet toegang zouden krijgen tot alle rolgegevens uit het hele land, in de aanloop naar afschaffing – naar thans wordt verwacht in maart 2008 – van het verplichte procuraat.

Het CBP oordeelde dat deze toegang bovenmatig zou zijn (niet in overeenstemming met artikel 11 Wbp) en dat advocaten alleen toegang zouden mogen hebben tot hun eigen zaken.<sup>53</sup> De Raad voor de Rechtspraak paste het beleid daarop aan. De toegang tot [www.roljournaal.nl](http://www.roljournaal.nl) is afgebakend.<sup>54</sup>

## 2.8 Beveiliging

Artikel 13 Wbp verplicht bestuursorganen tot het nemen van adequate beveiligingsmaatregelen. De laatste volzin van artikel 13 Wbp roept verantwoordelijken op om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen, als essentieel onderdeel van elke beveiligingsstrategie.

Actieve openbaarmaking van persoonsgegevens op internet brengt extra grote risico's met zich mee. Dat komt enerzijds door het onbekende aantal personen wereldwijd dat de gegevens kan opvragen en anderzijds door de onbekende verwerkingstermijn – de gegevens kunnen jaren na dato door een bezoeker weer elders op internet worden geplaatst of op andere wijze worden hergebruikt.

Bestuursorganen dienen daarom een aantal technische maatregelen te treffen om de persoonsgegevens op de aanvraagformulieren en beschikkingen te beveiligen tegen onrechtmatige verwerkingen.

1. Scherm de publicatie af voor zoekmachines. Een publicatie die voldoet aan de Wbp kan er toch toe bijdragen dat een betrokkene in zijn persoonlijke levenssfeer wordt geschaad, doordat via zoekmachines derden allerlei intieme details over deze betrokkene kunnen koppelen. Afscherming van persoonsgegevens voor zoekmachines is een heel eenvoudige, algemeen toepasbare en kosteloze stap om de kans op onrechtmatige verwerking door derden te verkleinen. Alle grote zoekmachines bieden handleidingen aan verantwoordelijken voor publicaties met behulp waarvan zij kunnen voorkomen dat een website of onderdelen uit een publicatie geïndexeerd of gearchiveerd worden.<sup>55</sup> Zonder een dergelijke maatregel ontstaan er grote risico's voor betrokkenen, waardoor de publicatie onrechtmatig kan zijn. Verantwoordelijken die de risico's willen vermijden van onrechtmatigheid, blokkeren daarom alle pagina's met persoonsgegevens voor zoekmachines. Dat kan door automatisch een anti-indexeringscode op te nemen in de onderliggende html.<sup>56</sup>
2. Maak het onmogelijk om te zoeken op naam of andere identificerende gegevens van een natuurlijk persoon, zowel rechtstreeks, via de eigen zoekfunctionaliteit als indirect, door zoekmachines van buiten.

---

<sup>53</sup> Het CBP deed hierover uitspraak in 2003, in z2002-01015. Na een heroverwegingsverzoek van de Raad voor de Rechtspraak herhaalde het CBP zijn uitspraak op 20 juni 2003, in z2003-0707.

<sup>54</sup> Zie URL: <http://www.rechtspraak.nl/Registers/Register+aangemelde+gegevensverwerkingen/#Roljournaal>: 'De gegevens kunnen, door advocaten die daartoe een wachtwoord hebben gekregen, alleen benaderd worden met een specifieke, door het College bescherming persoonsgegevens goedgekeurde, zoekvraag.'

<sup>55</sup> Wie zijn hele site wil afschermen voor alle zoekmachines, moet een documentje op de rootserver plaatsen met de naam 'robots.txt' met de volgende inhoud:

```
User-agent:
*Disallow: /
```

Hetzelfde principe kan worden toegepast op elke individuele webpagina, door aan de header van de pagina de code toe te voegen:

```
<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">.
```

<sup>56</sup> Dit is een algemene oplossing. Er bestaat ook een individuele oplossing, een constructie waarbij de betrokkene expliciet toestemming geeft voor toegang voor zoekmachines. Deze tweede mogelijkheid zal bij actieve openbaarmaking echter niet snel aan de orde zijn.

3. Maak massaal downloaden van alle documenten onmogelijk. Stel ook anderzins redelijke beperkingen aan de toegang, bijvoorbeeld het beperken van het aantal zoekvragen per IP-adres.
4. Beperkt de toegang tot de documenten tot de mensen voor wie de toegang noodzakelijk is. Als het om documenten gaat die voor een beperkte groep mensen toegankelijk dienen te zijn, zoals bijvoorbeeld een bepaalde groep bevoegde ambtenaren, zorg dan voor een toegangswijze die alleen hen toegang biedt, bijvoorbeeld door middel van een loginnaam-wachtwoord constructie.

Daarnaast dient het bestuursorgaan de specifieke beveiligingsrisico's te overwegen ten aanzien van elk soort persoonsgegevens dat hij op internet wil publiceren. Zo zal de publicatie op internet van 'natte' handtekeningen doorgaans niet mogelijk zijn gelet op de geringe meerwaarde van publicatie afgezet tegen het grote risico van identiteitsfraude waarmee zij gepaard gaat. Een handtekening is een persoonsgegeven als bedoeld in artikel 1 onder a Wbp. Door het publiceren van de 'natte' handtekening worden derden in staat gesteld op eenvoudige wijze deze signatuur te vervalsen. Juist door het publiceren op internet van persoonsgegevens in combinatie met de 'natte' handtekening wordt misbruik mogelijk gemaakt. In het geval van misbruik zal de betrokkene zich veel moeite moeten getroosten om te bewijzen dat niet hij, maar een (kwaadwillende) derde zijn persoonsgegevens heeft misbruikt, ongeacht of in theorie de bewijslast ligt bij degene die naar aanleiding van de handtekening de identiteit beoordeelt. Het CBP laat daarbij zwaar meewegen dat de Kamers van Koophandel hebben geconstateerd dat handtekeningen in toenemende mate worden gekopieerd met frauduleus oogmerk (zie kader). Het CBP acht identiteitsfraude een belangrijk maatschappelijk probleem dat noopt tot een zeer kritische (nadere) afweging van het belang van openbaarmaking via internet.

Zelfs als een bestuursorgaan toestemming heeft van betrokkenen om een integraal ingescand document online te publiceren, zou het bestuursorgaan om veiligheidsredenen af moeten zien van de publicatie van de handtekening op internet. Dit kan ook gelden ten aanzien van andere gegevens, zoals biometrische gegevens of anderszins zeer risicovolle gegevens. Ten aanzien van bijzondere persoonsgegevens, zoals gegevens over iemands gezondheid of politieke gezindheid, geldt sowieso dat het bestuursorgaan deze alleen met uitdrukkelijke toestemming van betrokkenen op internet mag publiceren.

#### **Geen handtekening publiceren op internet**

Op 1 mei 2007 trad een nieuwe wet in werking over het Handelsregister, met bepalingen over de elektronische ontsluiting van het register.<sup>57</sup> In de wet wordt een onderscheid gemaakt tussen de verplichte opname van sommige persoonsgegevens in het register en de publicatie ervan op internet. Het burgerservicenummer van natuurlijke personen die een onderneming hebben bijvoorbeeld wordt verplicht in het register opgenomen, maar mag niet aan derden worden verstrekt en dus niet op het internet worden gepubliceerd.

Tijdens de behandeling van het wetsvoorstel in de Tweede Kamer werd uitdrukkelijk gewezen op het risico van de publicatie op internet van de handtekening van in het handelsregister opgenomen natuurlijke personen. Uit de toelichting bij het amendement van Kamerlid Van Dijk: De Kamers van Koophandel constateren in toenemende mate dat handtekeningen worden gekopieerd met frauduleus oogmerk. Daarbij wordt onder meer gebruik gemaakt van de handtekening in het handelsregister zoals deze via internet kan worden ingezien. Om dergelijke fraude zo veel mogelijk te voorkomen is het gewenst dat handtekeningen van natuurlijke per-

<sup>57</sup> Wet van 22 maart 2007, Regels omtrent een basisregister van ondernemingen en rechtspersonen (Handelsregisterwet 2007), Staatsblad 153, 1 mei 2007.

sonen niet langer via internet worden getoond. Dat werpt een naar verwachting van de Kamers effectieve drempel op tegen het kopiëren van handtekeningen.<sup>58</sup> De staatssecretaris van Economische Zaken nam het amendement meteen over.

➤ NA PUBLICATIE

## 2.9 Verwijderen van onrechtmatigheden

Ook nadat de publicatie op internet is verschenen, moeten verantwoordelijken zich inspannen om aan de Wbp te blijven voldoen. Een publicatie die rechtmatig was doordat een betrokkene daarmee had ingestemd, wordt onrechtmatig op het moment dat de betrokkene zijn toestemming intrekt (zie paragraaf 2.4.1) of een terecht beroep doet op zijn recht van verzet (zie paragraaf 3.4). Persoonsgegevens die bij publicatie juist en nauwkeurig waren, kunnen na verloop van tijd niet meer kloppen en een onvolledig beeld schetsen (zoals: aan X is een vergunning geweigerd, terwijl de vergunning inmiddels naar aanleiding van een bezwaar- of beroepsprocedure alsnog is verleend).

Het is ook mogelijk dat een verantwoordelijke er pas nadat hij gegevens openbaar maakt heeft achter komt dat de openbaarmaking niet rechtmatig was, bijvoorbeeld omdat hij zich ten onrechte op een bepaalde rechtvaardigingsgrond meende te kunnen beroepen. In dat geval dienen de openbaar gemaakte gegevens terstond van internet verwijderd te worden.

---

<sup>58</sup> Kamerstukken II, 2006–2007, 30656, nr. 20, blz 7, 12 februari 2007.

## 3 Rechten van betrokkenen

### 3.1 Inleiding

Betrokkenen, de natuurlijke personen over wie persoonsgegevens worden gepubliceerd, kunnen ingrijpend benadeeld worden door de onjuiste, onvolledige of onnodige openbaarmaking van persoonsgegevens. Op grond van een enkel gegeven kunnen gemakkelijk foute conclusies worden getrokken. Oppervlakkige beeldvorming kan mensen schade berokkenen in hun maatschappelijk en persoonlijk functioneren. Bovendien kan openbaarmaking van persoonsgegevens ertoe bijdragen dat betrokkenen slachtoffer worden van criminele activiteiten, zoals oplichting en identiteitsfraude.

Verantwoordelijken hebben de plicht om te voldoen aan verzoeken van betrokkenen tot inzage en aan verzoeken tot verwijdering, verbetering, aanvulling of afscherming van persoonsgegevens als die feitelijk onjuist zijn, voor het doeleinde onvolledig of niet ter zake dienend, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.<sup>59</sup> Bij wet ingestelde openbare registers vormen hierop overigens een belangrijke uitzondering, zie voor meer daarover paragraaf 2.4.2.1 onder 2.

### 3.2 Inzage

Betrokkenen hebben een recht op inzage in de persoonsgegevens die over hen verwerkt worden. Bij actieve openbaarmaking geldt dat de meeste verwerkingen openbaar en kosteloos toegankelijk zijn. De betrokkene hoeft zich daarom meestal niet eerst met een formeel inzageverzoek tot de verantwoordelijke te wenden alvorens een gericht verwijderings- of verbeteringsverzoek te kunnen sturen.

Het inzagerecht is vooral van belang bij openbaarmaking op een wijze die niet automatisch ook toegankelijkheid voor de betrokkene inhoudt. Denk daarbij aan openbaarmaking via internet aan een beperkte groep ontvangers, of aan het ten behoeve van hergebruik op een gegevensdrager verstrekken van persoonsgegevens aan een ontvanger.

Op grond van de informatieplicht uit de artikelen 33 en 34 Wbp dienen verantwoordelijken de betrokkenen voorafgaand aan de publicatie mee te delen welke soorten persoonsgegevens er over hen op welke wijze worden gepubliceerd en met welk doel.<sup>60</sup> De betrokkene heeft het recht zich 'vrijelijk' (dus zonder nadere motivering) en 'met redelijke tussenpozen' tot de verantwoordelijke te wenden met een inzageverzoek.<sup>61</sup> Het verzoek om kennisneming mag echter niet ongericht zijn.<sup>62</sup> De verantwoordelijke moet binnen vier weken schriftelijk reageren. Dat mag ook elektronisch.<sup>63</sup> Het CBP oordeelde in 2003<sup>64</sup> dat een ieder zonder voorbehoud het recht heeft kennis te nemen van de verwerking van zijn persoonsgegevens. Een bericht op grond van art. 35 Wbp moet een volledig en begrijpelijk overzicht zijn van de gegevens die over een betrokkene worden verwerkt. Het gaat daarbij niet om een beschrijving of samenvatting van de gegevens, maar om een volledige weergave. Als de gegevens onvolledig zijn, is de betrokkene immers onvoldoende in staat zijn rechten op grond van de Wbp te effectueren.<sup>65</sup> De verantwoordelijke mag bij zeer algemene verzoeken om inzage wel om precisering vragen, om een oneven-

---

<sup>59</sup> Zie voor een algemene toelichting het informatieblad 'Rechten van de betrokkene'. Het CBP heeft daarnaast specifieke informatiebladen over correctie en inzage, zowel voor betrokkenen als verantwoordelijken. De informatiebladen zijn beschikbaar via de website van het CBP, URL: <http://www.cbpweb.nl>, onder 'nieuws en publicaties', 'publicaties', 'informatiebladen'.

<sup>60</sup> Zie hierover verder paragraaf 2.5.

<sup>61</sup> Art. 35, eerste lid Wbp.

<sup>62</sup> MvT, blz. 44.

<sup>63</sup> Kamerstukken II, nr. 8, blz. 27.

<sup>64</sup> CBP, z2003-01617. URL: [http://www.cbpweb.nl/documenten/med\\_uit\\_z2003-1617.shtml](http://www.cbpweb.nl/documenten/med_uit_z2003-1617.shtml).

<sup>65</sup> Deze interpretatie is medio 2007 bevestigd door de Hoge Raad in de uitspraken over de Dexia-zaak, Hoge Raad, 29 juni 2007, LJN: AZ4663 en Hoge Raad, 29 juni 2007, LJN: AZ4664.

redige administratieve inspanning te vermijden. De verantwoordelijke moet bovendien zorgen voor een 'deugdelijke vaststelling van de identiteit van de verzoeker' (artikel 37 Wbp), bijvoorbeeld door een kopie te vragen van een identiteitsbewijs, om te voorkomen dat persoonsgegevens in verkeerde handen belanden. De verantwoordelijke mag voor een inzageverzoek maximaal 0,23 eurocent per pagina vragen, met een maximum van 4,50 euro.<sup>66</sup> Deze vergoeding moet worden terugbetaald als de verantwoordelijke na de inzage een verbeterings-, vewijderings-, aanvullings- of afschermingsverzoek moet honoreren.

### **3.3 Correctie en verwijdering**

Betrokkenen hebben een breed recht op correctie. Ze mogen verantwoordelijken op grond van artikel 36 Wbp verzoeken om verbetering, aanvulling, verwijdering of afscherming van gegevens indien ze feitelijk onjuist zijn of voor het doeleinde onvolledig of niet ter zake dienend, dan wel anderszins in strijd met een wettelijk voorschrift worden gepubliceerd. Als het verzoek terecht is, dient de verantwoordelijke hieraan gehoor te geven. Verantwoordelijken moeten een eventuele weigering tot het corrigeren, aanvullen, afschermen of verwijderen van gegevens met redenen omkleden.

### **3.4 Recht van verzet**

Op grond van artikel 40 Wbp kunnen betrokkenen zich verzetten tegen de publicatie van hen betreffende persoonsgegevens op internet op grond van hun bijzondere persoonlijke omstandigheden. Dit relatieve recht van verzet is alleen van toepassing op verwerkingen op grond van artikel 8 onder e en f.

Betrokkenen kunnen het bestuursorgaan zowel op voorhand als naderhand vragen om geen of alleen bepaalde persoonsgegevens over hen op internet te publiceren. Het bestuursorgaan dient vervolgens bij elk verzoek te beoordelen of het verzet gerechtvaardigd is.

Een betrokkene wiens gegevens op grond van artikel 8 onder e Wbp op internet worden gepubliceerd kan de verantwoordelijke vragen om op grond van zijn bijzondere persoonlijke omstandigheden af te zien van publicatie van (een deel van) de gegevens. Bijvoorbeeld in het geval van publicatie door een gemeente van het adres, een omschrijving van de vergunning en de bouwtekening bij aanvraag van een bouwvergunning, kan de betrokkene de gemeente vragen af te zien van publicatie van de bouwtekening, bijvoorbeeld met het argument dat het publiceren van de bouwtekening voor deze verbouwing tot een duidelijke grotere kans op inbraak zou leiden.

Zowel ten aanzien van artikel 36 Wbp als ten aanzien van artikel 40 Wbp dient het bestuursorgaan heel duidelijk te maken op welke wijze(n) een betrokkene zich kan verzetten (langs welke kanalen), zowel op voorhand als naderhand.

### **3.5 Besluiten in de zin van de Awb**

Artikel 45 Wbp bepaalt dat beslissingen van bestuursorganen over een aantal rechten die de Wbp toekent aan betrokkenen gelden als besluiten in de zin van artikel 1:3 van de Algemene wet bestuursrecht. Voor zover hier relevant gaat het over inzageverzoeken, verzoeken tot het verbeteren, aanvullen, verwijderen of afschermen van gegevens en het aantekenen van verzet in verband met bijzondere persoonlijke omstandigheden. Als een betrokkene vraagt om verwijdering van zijn gegevens, en het bestuursorgaan weigert dit, dan kan de betrokkene op grond van de Awb bezwaar aantekenen tegen deze weigering en in beroep gaan na eventuele afwijzing van zijn bezwaar. Als de betrokkene een dringend belang heeft bij onmiddellijke verwijdering, dan kan hij een voorlopige voorziening vragen bij de bestuursrechter. Bezwaar en beroep staat ook open tegen de weigering om een besluit te nemen, net als het niet tijdig nemen van een besluit, of het niet volledig voldoen aan een verzoek (op te vatten als gedeeltelijke weigering).

---

<sup>66</sup> Artikel 39 Wbp en het bijbehorende Besluit Kostenvergoeding rechten betrokkene Wbp van 13 juni 2001.

## **4 Handhaving en de rol van het CBP**

### **4.1 Inleiding**

Verantwoordelijken die in strijd handelen met het bepaalde in de Wbp kunnen op verschillende manieren in rechte worden aangesproken, zowel civielrechtelijk, bestuursrechtelijk als strafrechtelijk. Betrokkenen hebben een aantal mogelijkheden om zelf hun recht te halen, zowel op grond van de Wbp, als op grond van het algemene bestuursrecht en op grond van het civiel recht. Daarnaast heeft het CBP als toezichthouder een aantal bestuursrechtelijke mogelijkheden om te handhaven op het bepaalde in de Wbp.

### **4.2 Maatregelen door betrokkenen**

Een betrokkene die meent dat zijn persoonsgegevens onrechtmatig worden gepubliceerd op internet, kan actie ondernemen door het recht uit te oefenen op inzage, correctie, verwijdering en verzet (zie het vorige hoofdstuk). Het CBP heeft op [www.mijnprivacy.nl](http://www.mijnprivacy.nl) concrete hulpmiddelen voor betrokkenen gepubliceerd, in de vorm van onder meer voorbeeldbrieven aan verantwoordelijken en gerichte vragen en antwoorden over verschillende soorten internetpublicaties.

Als de verantwoordelijke niet reageert of weigert om aan een verzoek te voldoen, kan een betrokkene naar de rechter gaan met een beroep op de rechtsbescherming die de Wbp biedt. Een betrokkene kan daarnaast op basis van het gewone recht een vordering indienen, bijvoorbeeld op grond van een onrechtmatige daad.

#### **4.2.1 Rechtsbescherming onder de Wbp**

Als een verantwoordelijke zich niet houdt aan het bepaalde in de Wbp, kan een betrokkene de rechter vragen om hem een schadevergoeding toe te kennen (artikel 49 Wbp) of om een verbod op te leggen op het verder verwerken van bepaalde persoonsgegevens (artikel 50 Wbp).

De Wbp biedt betrokkenen daarnaast in een aantal specifieke gevallen (onder andere bij weigering van inzage in persoonsgegevens en bij weigering van een verzoek tot verbetering, aanvulling of verwijdering van gegevens) de laagdrempelige mogelijkheid een verzoekschrift in te dienen bij de rechtbank, mits de verantwoordelijke een bedrijf of een burger is. Bij actieve openbaarmaking is de verantwoordelijke doorgaans echter een bestuursorgaan. In dat geval zijn de bezwaar- en beroepsregels uit de Algemene wet bestuursrecht van toepassing.

#### **4.2.2 Andere rechtsmiddelen voor betrokkenen**

Publicaties die in strijd zijn met een of meer bepalingen uit de Wbp zijn mogelijk ook onrechtmatig op andere gronden. Een betrokkene heeft in dergelijke gevallen, naast de mogelijkheden van de Wbp, nog een aantal andere mogelijkheden om zijn recht te halen. Een betrokkene kan een verantwoordelijke bijvoorbeeld voor de rechter dagen op grond van een onrechtmatige daad (artikel 6:162 Burgerlijk Wetboek). Via een dergelijke civiele procedure kan een betrokkene staking van de publicatie vorderen, evenals verwijdering van gegevens, vergoeding van materiële en immateriële schade en vergoeding van proceskosten. De betrokkene kan de rechter vragen om aan de veroordeling een dwangsom te verbinden.

### **4.3 Handhaving door het CBP**

Het CBP heeft de wettelijke taak om toe te zien op de naleving van de Wbp (artikel 51 Wbp). Daartoe heeft het CBP een aantal middelen, variërend van bemiddeling tot het opleggen van een last onder dwangsom.

#### **4.3.1 Bemiddeling, klachtbehandeling en ambtshalve onderzoek**

Het CBP kan bemiddelen bij geschillen over onder andere het verkrijgen van inzage in persoonsgegevens en het verbeteren, aanvullen, verwijderen of afschermen van persoonsgegevens (artikel 47 Wbp). Ook kan het CBP op grond van een klacht van een belanghebbende of op eigen initiatief een onderzoek instellen naar de naleving van de Wbp (artikel 60 Wbp).

Daarbij kan het CBP zijn toezichthoudende bevoegdheden inzetten<sup>67</sup>, waarbij een verantwoordelijke verplicht is alle gevraagde medewerking te verlenen. Het CBP kan inlichtingen vorderen, inzage vorderen in zakelijke gegevens, zaken en middelen onderzoeken (waaronder computerapparatuur) en mag ruimtes betreden, waaronder ook woningen.<sup>68</sup>

Het aantal aangedragen zaken en de complexiteit daarvan neemt echter voortdurend toe, terwijl de middelen die het CBP ter beschikking staan begrensd zijn. Het CBP kan derhalve niet alle zaken die worden aangebracht in behandeling nemen en moet keuzes maken. Bij klachten gebeurt dit aan de hand van criteria zoals de ernst van de overtreding, de mate van concreetheid van de aanwijzingen, een inschatting van de juridische haalbaarheid en de door het CBP te investeren capaciteit en menskracht, maar vooral ook de verwachting over de potentiële preventieve werking die van handhaving in een specifiek geval zal uitgaan.<sup>69</sup>

#### **4.3.2 Bestuursdwang en last onder dwangsom**

Indien de Wbp niet wordt nageleefd kan het CBP bestuursdwang toepassen. Onder bestuursdwang wordt verstaan het met feitelijk handelen optreden door een bestuursorgaan tegen een illegale situatie, doorgaans op kosten van de overtreder. Ook kan het CBP een last onder dwangsom opleggen. Een last onder dwangsom kan bijvoorbeeld inhouden dat een verantwoordelijke een gegevensverwerking moet aanpassen of staken op straffe van een dwangsom van een bepaald bedrag per dag. Als de verantwoordelijke niet voldoet aan de last, kan het te betalen geldbedrag fors oplopen, tot een vooraf vastgesteld maximumbedrag.

#### **4.3.3 Strafrechtelijke handhaving**

Een verantwoordelijke riskeert ten slotte ook nog strafrechtelijke sancties, onder meer voor overtreding van de meldingsplicht (artikel 27 en 28 jo. 75 Wbp).

#### **4.3.4 Internationaal toezicht**

Het CBP werkt bij onderzoek naar overtredingen van de Wbp op internet samen met collega-toezichthouders uit andere landen binnen en buiten de EU. De toezichthouders binnen de Europese Unie zijn wettelijk verplicht om elkaar desgevraagd bijstand en medewerking te verlenen, voor zover dat noodzakelijk is voor de uitvoering van onderzoeken naar publicaties op internet die door hen worden behandeld.

---

<sup>67</sup> Voor al zijn toezichthoudende activiteiten, niet alleen bij ambtshalve onderzoeken.

<sup>68</sup> Artikel 61 tweede lid Wbp jo. artikel 5:15 Awb.

<sup>69</sup> Zie ook de Uitgangspunten en beleidsregels werkwijze CBP, Staatscourant, 4 oktober 2004, nr. 190.

## 5 Managementsamenvatting

De overheid kent een lange traditie van openbaarheid van bepaalde gegevensbestanden, zoals het kadaster en het handelsregister. De afgelopen decennia is er daarnaast ook steeds meer aandacht voor openbaarheid van bestuur. Het afgelopen decennium is de aandacht steeds meer verschoven van passieve naar *actieve* openbaarmaking, dat wil zeggen: informatieverschaffing uit eigener beweging. Het middel dat daarvoor gehanteerd wordt is steeds vaker publicatie op internet.

Publicaties op internet zijn over het algemeen wereldwijd, 24 uur per dag, toegankelijk voor een potentieel zeer omvangrijk en divers publiek. Het voordeel van deze grote toegankelijkheid heeft als keerzijde dat mensen van wie persoonsgegevens op internet staan, de betrokkenen, grote nadelen kunnen ondervinden van onjuiste, onvolledige of onnodige publicatie van hun persoonsgegevens.

Actief openbaar gemaakte persoonsgegevens moeten op dezelfde zorgvuldige wijze worden verwerkt als passief openbaar gemaakte persoonsgegevens. Sterker nog: gelet op de extra risico's waarmee actieve openbaarmaking op internet gepaard gaat, dient daarbij extra terughoudendheid te worden betracht. Deze publicatie van het College bescherming persoonsgegevens verschaft bestuursorganen duidelijkheid over het toepassen van de Wet bescherming persoonsgegevens (Wbp) bij actieve openbaarmaking, met een focus op actieve openbaarmaking via internet.

### Regels

In het kort dienen overheidsinstellingen die persoonsgegevens actief openbaar (willen) maken, de verantwoordelijken, zich te houden aan de volgende regels.

#### Voorafgaand aan publicatie

1. Stel vast of de openbaarmaking een legitiem doeleinde dient en of dat doel verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verkregen.
2. Beschik over een rechtvaardigingsgrond voor openbaarmaking.  
De belangrijkste rechtvaardiging voor openbaarmaking door middel van publicatie op internet is dat deze noodzakelijk is voor de goede uitvoering van een publiekrechtelijke taak van het betreffende bestuursorgaan. De Wob biedt daarentegen slechts zelden een rechtvaardigingsgrond in de zin van een wettelijke verplichting tot actieve openbaarmaking door middel van publicatie op internet. In sommige gevallen kan de toestemming van de betrokken burgers, een wettelijke verplichting buiten de Wob of het gerechtvaardigd belang van het betreffende bestuursorgaan een rechtvaardigingsgrond vormen. Bij alle rechtvaardigingsgronden behalve toestemming moet telkens de noodzaak worden vastgesteld om de gekozen persoonsgegevens op internet te publiceren.
3. Publiceer geen bijzondere persoonsgegevens.  
Bijzondere persoonsgegevens zijn gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag. Ook wettelijk voorgeschreven identificatienummers zijn bijzondere persoonsgegevens. Publicatie van bijzondere persoonsgegevens op internet is alleen toegestaan als de betrokkene er uitdrukkelijk toestemming voor heeft gegeven of de gegevens bewust zelf openbaar heeft gemaakt.

#### Tijdens publicatie

4. Leef de informatieplicht na.  
Verantwoordelijken dienen betrokkenen actief te informeren over het doel en de opzet van de publicatie.
5. Vermeld duidelijk uw eigen identiteit, toegankelijk voor iedere bezoeker van de publicatie.

6. Zorg ervoor dat u persoonsgegevens niet langer bewaart en ter beschikking stelt dan strikt noodzakelijk.
7. Waarborg actief de kwaliteit en juistheid van de gepubliceerde persoonsgegevens.
8. Tref beveiligingsmaatregelen tegen onbevoegd gebruik.  
Onder die maatregelen vallen onder meer dataminimalisatie en het afschermen van persoonsgegevens voor zoekmachines.

### **Volgend op publicatie**

9. Voldoe aan verzoeken van betrokkenen tot inzage en aan verzoeken tot verwijdering, verbetering, aanvulling of afscherming van persoonsgegevens als die feitelijk onjuist zijn, voor het doeleinde onvolledig of niet ter zake dienend, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Verwijder gegevens tevens als de betrokkene zijn toestemming voor publicatie intrekt.
10. Verwijder onrechtmatig gepubliceerde persoonsgegevens.

### **Sancties**

Verantwoordelijken die zich niet houden aan de Wbp kunnen door betrokkenen in rechte worden aangesproken, zowel op grond van de Wbp als op grond van het bestuursrecht en het civiele recht. Daarnaast kunnen zij in aanraking komen met de toezichthoudende bevoegdheden van het College bescherming persoonsgegevens, variërend van bemiddeling tot het instellen van een ambtshalve onderzoek en het opleggen van een dwangsom.

## Bijlage 1

Deze bijlage bevat de belangrijkste constatering en aanbevelingen over de bescherming van persoonsgegevens bij actieve openbaarmaking door de Raad van Europa (gebaseerd op het Europees gegevensbeschermingsverdrag) en de Artikel 29 Werkgroep (gebaseerd op Richtlijn 95/46/EG). Zie verder paragraaf 1.8.

### Raad van Europa

De Raad van Europa benoemt in zijn *Recommendation No. R (91) 10 of the Committee of Ministers to Member States on the Communication of third parties of personal data held by public bodies* de volgende risico's van het elektronisch opslaan en verspreiden van persoonsgegevens door openbare instellingen:

- het biedt de mogelijkheid om langs elektronische weg profielen op te stellen van mensen, bijvoorbeeld over hun gezinssamenstelling of hun financiële situatie;
- het opent de mogelijkheid van het zoeken naar gegevens over een persoon in allerlei openbare bestanden van verschillende aard;
- het maakt het gebruik van openbare gegevens mogelijk voor andere doeleinden dan waarvoor ze verzameld en bewaard zijn.

De Raad formuleert vervolgens onder meer de onderstaande principes:

- Principe 2.3: Als een derde persoonsgegevens verwerkt verkregen van een openbare instelling, dan moet op die verwerking de wetgeving ter bescherming van persoonsgegevens van toepassing zijn.
- Principe 4.3: Als een openbare instelling gegevens openbaar maakt, dan moet zij daarbij de mogelijkheid hebben om gegevens uit te zonderen van betrokkenen wier veiligheid of privacy in het bijzonder in het geding is.
- Principe 5.1: Er moeten specifieke regels zijn voor het elektronisch opslaan en raadplegen van openbare informatie.
- Principe 5.2: Er moeten technische middelen ingezet worden om het ongeoorloofd raadplegen of downloaden van openbare informatie tegen te gaan.<sup>70</sup>
- Principe 6.3: Als een derde persoonsgegevens verwerkt verkregen van een openbare instelling, dan moet een betrokkene alle gebruikelijke rechten hebben, zoals op informatie, raadpleging, verzoek om correctie, verwijdering. Het recht op verwijdering moet daarbij niet relatief, maar absoluut zijn.<sup>71</sup>
- Principe 7: Het combineren van uit openbare bronnen verkregen gegevens moet niet zijn toegestaan, tenzij dit bij wet is geregeld en er adequate waarborgen zijn.

### Artikel 29 Werkgroep

Het *Advies 3/99 betreffende Overheidsinformatie en de bescherming van persoonsgegevens* van de Artikel 29 Werkgroep is een reactie op een groenboek van de Europese Commissie over het beter toegankelijk maken van overheidsinformatie. Het bevat de volgende kernpunten en -overwegingen:

- Het elektronisch ontsluiten van openbare gegevens brengt de volgende risico's met zich mee: 'cross searching'; profilering; bestandskoppeling, i.h.b. data mining / data warehousing.
- De wettelijke regels inzake de bescherming van persoonsgegevens zijn onverkort van toepassing op openbaar gemaakte persoonsgegevens.<sup>72</sup>

---

<sup>70</sup> Dit principe ziet met name op grootschalig downloaden.

<sup>71</sup> Dit principe is een uitwerking van Principe 2.3.

<sup>72</sup> "Onze wetten inzake gegevensbescherming op openbaar gemaakte persoonsgegevens van toepassing verklaren, is overigens overbodig omdat dit uit de wetsteksten blijkt: een persoonsgege-

- Technische en organisatorische maatregelen kunnen ertoe bijdragen – zonder een waterdichte bescherming te pretenderen – dat het openbaarmaking geschiedt conform de regels voor gegevensbescherming, in het bijzonder het beginsel van doelbinding. (De in het groenboek gebezigde term “publicly available” is dan ook ongelukkig, beter zou bijvoorbeeld “publicly accessible” zijn.)
- Voorbeelden van technische en organisatorische maatregelen t.b.v. naleving gegevensbeschermingsregels, i.h.b. doelbinding:
  - ♦ niet alle gegevens op internet zetten: slechts een deel van de *records* en/of slechts een deel van de *attributen* per record.
  - ♦ gegevens slechts voor bepaalde tijd op internet zetten;
  - ♦ gegevens alleen beschikbaar stellen aan de wettelijk beoogde doelgroep of aan wie een belang kan aantonen;
  - ♦ gebruik van de gegevens, bijv. voor commerciële doeleinden of in de media, beperken;
  - ♦ beperken toegang d.m.v. zoekcriteria – uitgangspunt: iedereen mag alle individuele gegevens lezen, maar niemand alle gegevens als geheel.
- Ingevolge overweging 58 van de richtlijn mag niet de totaliteit van gegevens in een register worden doorgegeven naar een derde land, maar mag de doorgifte slechts plaatsvinden op verzoek van de personen die hierbij een rechtmatig belang hebben.<sup>73</sup>

---

ven blijft een persoonsgegeven, ook al is het openbaar gemaakt, en wordt daarom beschermd. Dit betekent echter wel dat moet worden bepaald hoe openbaar gemaakte persoonsgegevens moeten worden beschermd. Richtlijn 95/46/EG biedt hiervoor een aantal antwoorden.”

<sup>73</sup> (58) Overwegende dat onder bepaalde omstandigheden [...] afwijkingen van dit verbod moeten kunnen worden toegestaan, wanneer [...] het gaat om een doorgifte uit een bij de wet ingesteld register dat bedoeld is voor raadpleging door het publiek of personen met een gerechtvaardigd belang; dat bij een dergelijke doorgifte niet de totaliteit van de in dit register opgenomen gegevens of categorieën gegevens zou mogen worden verstrekt; dat wanneer een register bedoeld is voor raadpleging door personen met een gerechtvaardigd belang, de doorgifte slechts zou moeten kunnen plaatsvinden op verzoek van deze personen of wanneer de gegevens voor hen zijn bestemd.

## Bijlage 2 – Wettelijke verplichtingen tot actieve openbaarmaking

In sommige gevallen kunnen verantwoordelijken het moeten nakomen van een wettelijke verplichting aanvoeren als rechtvaardigingsgrond voor actieve openbaarmaking. In paragraaf 2.4.2.2 zijn hun mogelijkheden daartoe aangegeven aan de hand van drie wettelijke kaders voor openbaarmaking van gegevens. In deze bijlage worden die drie kaders en de bijbehorende verplichtingen tot openbaarheid in meer detail geanalyseerd.

Het moeten nakomen van een wettelijke verplichting is een rechtvaardigingsgrond die naar verwachting in de toekomst steeds vaker door overheidsinstellingen of beheerders van openbare registers gebruikt kan worden voor actieve openbaarmaking, en in het bijzonder actieve openbaarmaking via internet. Er is veel wetgeving in ontwikkeling ter bevordering van de transparantie en eenvormigheid van de besluitvorming door bestuursorganen. Daarbij wordt elektronische publicatie van persoonsgegevens soms expliciet voorgeschreven.

Er zijn op hoofdlijnen drie wettelijke kaders voor openbaarmaking te onderscheiden:<sup>74</sup>

- A. Openbaarmaking op grond van specifieke wetgeving voor de verwerking van gegevens:
  - 1. specifieke wetgeving die een uitputtend regime bevat voor de verwerking van persoonsgegevens en de toepasselijkheid van de Wbp expliciet uitsluit;
  - 2. specifieke wetgeving die een regeling op deelterreinen van de bescherming van persoonsgegevens bevat en waarbij de Wbp aanvullend van toepassing is.
- B. Openbaarmaking op grond van generieke wetgeving voor de verwerking van gegevens, te weten de Wob.

Bij het onder A genoemde kader kunnen nog worden onderscheiden:

Welk van deze kaders ook aan de orde is, telkens zal moeten worden nagegaan of er inderdaad sprake is van een wettelijke mogelijkheid c.q. verplichting tot *actieve* openbaarmaking of slechts van een mogelijkheid c.q. verplichting tot openbaarmaking op zich. Zoals hieronder nog nader zal worden toegelicht is er in dat laatste geval in beginsel geen grondslag voor actieve openbaarmaking. Aangezien er nog nauwelijks expliciete wettelijke verplichtingen tot actieve openbaarmaking bestaan zal in de rest van deze paragraaf dan ook blijken dat wettelijke verplichtingen in ieder geval momenteel nog zelden de actieve openbaarmaking van persoonsgegevens kunnen rechtvaardigen.

### *A. Openbaarmaking op grond van specifieke wetgeving*

Allereerst bekijken we openbaarmaking op grond van specifieke wetgeving voor de verwerking van gegevens. Zoals hierboven al is aangegeven valt deze uiteen in twee relevante deelregimes, te weten:

- 1. specifieke wetgeving die een uitputtend regime bevat voor de verwerking van persoonsgegevens en de toepasselijkheid van de Wbp expliciet uitsluit;
- 2. specifieke wetgeving die een regeling op deelterreinen van de bescherming van persoonsgegevens bevat en waarbij de Wbp aanvullend van toepassing is.

De MvT bij de Wbp verwoordt dit onderscheid als volgt (blz. 12):

Om normen per sector in formele wetgeving te concretiseren, kunnen twee modellen worden onderscheiden. Het ene is dat waarbij bepaalde regels in een bijzondere wet worden opgenomen, en waarbij de WBP als algemene wet van toepassing is op de gebieden die niet geregeld zijn. In dit model zijn in de betreffende sector in beginsel zowel de WBP als de bijzondere wet van toepassing. De andere is het model waarbij voor een sector een uitputtend (privacy-)regime is geschapen en waarbij in de wet wordt vermeld dat de toepasselijkheid van de algemene regels geheel

---

<sup>74</sup> Naast de in paragraaf 2.4.2.1 behandelde noodzaak voor de goede vervulling van een publiek-rechtelijke taak.

wordt uitgesloten. In beide modellen moeten de regels, voor zover zij onder het communautaire recht vallen, in overeenstemming zijn met de richtlijn.

#### 1. Specifieke wetgeving met een uitputtend regime

Het eerste deelregime betreft specifieke wetgeving die een uitputtend regime bevat voor de verwerking van persoonsgegevens en de toepasselijkheid van de Wbp expliciet uitsluit. Vanwege het vereiste dat de Wbp uitdrukkelijk wordt uitgesloten is het helder welke wetten onder dit deelregime vallen. Er zijn naast de Wbp zelf geen wetten waarin de Wbp expliciet wordt uitgesloten, zodat het hier alleen de verwerkingen betreft die zijn uitgezonderd in artikel 2 Wbp. Concreet gaat het dan om verwerkingen van persoonsgegevens gebaseerd op de onderstaande wetten:

- de Wet op de inlichtingen- en veiligheidsdiensten 2002 en de Wet veiligheidsonderzoeken;
- de Wet politiegegevens;
- de Wet gemeentelijke basisadministratie persoonsgegevens;
- de Wet justitiële en strafvorderlijke gegevens;
- de Kieswet.

Wat betreft het wettelijk kader voor actieve openbaarmaking is dit de eenvoudigste categorie. Immers, de specifieke wetgeving beoogt een *uitputtend* regime te geven voor de betreffende gegevensverwerkingen. In het bijzonder is actieve openbaarmaking van gegevens uit deze verwerkingen dan ook slechts mogelijk voor zover daarin in de betreffende wet is voorzien.<sup>75</sup>

#### FOTO'S VAN VERDACHTEN OP INTERNET

In 2005 is het CBP een ambtshalve onderzoek gestart naar de rechtmatigheid van het publiceren van foto's van verdachten op het internet: de politie Rotterdam Rijnmond plaatste naar aanleiding van de ernstige voetbalrellen rondom de wedstrijd Feyenoord-Ajax op 17 april foto's van onbekende verdachten op internet. Ook onderzocht het CBP publicatie van foto's door de politie Gelderland Zuid (Nijmegen) naar aanleiding van rellen rond de Vierdaagse, en het voornemen van de politie Hollands-Midden om foto's van verdachten van geweldpleging tegen politieagenten tijdens de Katwijkse kermis op internet te publiceren.<sup>76</sup>

In de conclusie van het onderzoek naar de handelswijze van politie en justitie in Rotterdam, Nijmegen en Katwijk, waarbij hetzelfde middel in verschillende zaken werd ingezet dan wel inzet daarvan werd overwogen, benadrukt het CBP het belang van een zorgvuldige, evenwichtige afweging van belangen. Bij het publiceren van foto's van verdachten op internet dient er in ieder afzonderlijk geval een afweging te worden gemaakt of het opsporingsbelang opweegt tegen de ingrijpende maatregel van publicatie op internet. Daarbij moeten ook de mogelijk beschadigende en onomkeerbare neveneffecten van publicatie op internet voor de verdachten, met name voor 'first offenders' (iemand die voor het eerst met de politie in aanraking komt), zorgvuldig worden meegewogen.

De Wet politieregisters (Wpolr) kende een gesloten verstrekkingenregime, dat wil zeggen dat persoonsgegevens uit een politieregister niet verstrekt konden worden

<sup>75</sup> De Wob biedt geen grondslag voor openbaarmaking uit de hier behandelde verwerkingen, gelet op de beperking "onverminderd het elders bij wet bepaalde" bij de verplichting tot informatieverstrekking uit artikel 2 lid 1 Wob en de uitputtende strekking van de gegevensverwerkingsregimes in de betreffende wetten.

<sup>76</sup> College bescherming persoonsgegevens, z2005-0844, 3 mei 2006, URL: [http://www.cbprecht.nl/documenten/uit\\_z2005-0844.shtml](http://www.cbprecht.nl/documenten/uit_z2005-0844.shtml)

aan derden tenzij dit uitdrukkelijk bepaald was in een wet of besluit. In casu was de uitzondering van artikel 30 Wpolr toepasbaar op het verstrekken van foto's van verdachten in de vorm van publicatie op internet. Artikel 30 Wpolr bepaalde dat in incidentele gevallen met het oog op de politietaak voortvloeiend uit artikel 2 Politiewet de geheimhoudingsplicht opzij gezet kon worden en dat verstrekking aan derden mogelijk was. Er moest wel voldaan zijn aan de eisen van proportionaliteit en subsidiariteit.

*N.B. Op 1 januari 2008 is de Wet politieregisters vervangen door de Wet politiegegevens (Wpg). Artikel 19 Wpg bevat een verstrektingsregime dat vergelijkbaar is met het hierboven behandelde artikel 30 Wpolr. Wel zijn als extra voorwaarden toegevoegd dat met de verstrekking een zwaarwegend algemeen belang wordt gediend, en dat de beslissing tot verstrekking wordt genomen in overeenstemming met het bevoegde gezag. Aan beide voorwaarden zou in deze casus zijn voldaan.*

De Aanwijzing Opsporingsberichtgeving van het College Procureurs-Generaal schrijft voor hoe er gehandeld dient te worden bij het publiek maken van verdachten via de media. Onbekende verdachten kunnen via de media worden opgespoord als het gaat om een misdrijf waarvoor voorlopige hechtenis is toegestaan op grond van artikel 67 van het Wetboek van Strafvordering. Het CBP benadrukte in zijn conclusie dat als aan deze eerste voorwaarde is voldaan er een per individu een afweging gemaakt moet worden of de opsporing van de onbekende verdachte in verhouding staat tot de manier waarop dit gebeurt en de mogelijke consequenties daarvan.

## 2. Specifieke wetgeving met een regeling op deelterreinen

Het tweede deelregime betreft specifieke wetgeving die een regeling op deelterreinen van de bescherming van persoonsgegevens bevat en waarbij de Wbp aanvullend van toepassing is. Uit de Memories van Toelichting bij de Wbp en de Aanpassingswet<sup>77</sup> blijkt dat het gaat om een veelheid aan wetten (of delen daarvan), die regels stellen voor onder meer gegevensverwerkingen van het Kadaster, de RDW, het CBS en de Kamers van Koophandel (het Handelsregister). Andere voorbeelden zijn de Woningwet, die gemeenten verplicht tot het bijhouden van een register van verleende bouwvergunningen, en hoofdstuk 12 van de Wet milieubeheer, dat een aantal registratieverplichtingen bevat, alsmede regels over de openbaarheid ervan, ter implementatie van het verdrag van Aarhus.

De MvT bij de Aanpassingswet gaat in het bijzonder in op de gevolgen van het principe van doelbinding in deze context (blz. 3):

Hierboven is reeds aangegeven dat het voorschrift van doelspecificatie van artikel 6, eerste lid, onderdeel b, van de richtlijn in een aantal gevallen noodzaakt tot een nadere doelomschrijving in nationale wettelijke voorschriften. Zo wordt bijvoorbeeld in artikel 3a van de Kadasterwet (artikel 1 van hoofdstuk 7 van dit wetsvoorstel) en in artikel 2 van de Handelsregisterwet 1996 een nadere doelomschrijving voorgesteld van de in deze wetten geregelde openbare registers. Deze doelspecificatie is van belang voor de mogelijkheid van verstrekken van gegevens uit openbare registers. In paragraaf 9.3 van het algemeen deel van de memorie van toelichting bij de Wbp is opgemerkt dat, indien een openbaar register tot doel heeft informatie te geven, bij verstrekking van persoonsgegevens het achterliggende doel van het register medebepalend is voor de wijze van verstrekking. Deze beperking in de wijze van verstrekking, voortvloeiend uit het doel van een register (doelbinding) brengt met zich dat het bijvoorbeeld in strijd is met het doel van het handelsregister indien achtergronden van aan rechtspersonen verbonden natuurlijke personen zouden worden verschaft in vorm van overzichten op naam. Dit onverenigbaar gebruik is uitdrukkelijk uitgesloten in het voorgestelde artikel 15, tweede lid, van de Handelsregisterwet 1996.

<sup>77</sup> Wet tot wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens. Staatsblad 2002, 196.

Het doelbindingsvoorschrift heeft een reflexwerking op artikel 13 van de Wbp. Artikel 13 legt op de verantwoordelijke de plicht om bij voorbeeld bij ontsluiting van een openbaar register de gegevens adequaat te beveiligen tegen enige vorm van onrechtmatige verwerking. Dit legt beperkingen op aan de wijze waarop overzichten uit het register kunnen worden verstrekt, bijvoorbeeld via Internet of CD-ROM.

Vervolgens wordt in de MvT uitvoerig ingegaan op gegevensbeschermingsaspecten van met name enkele van de hierboven genoemde (al dan niet openbare) registers, met de daarbij behorende wettelijke bepalingen. Helaas is de wetgever in de Aanpassingswet bij zijn selectie van zowel relevante gegevensverwerkingen als relevante aspecten daarvan niet altijd even volledig geweest.<sup>78</sup> Ook de wetgevingspraktijk sindsdien laat een wisselend beeld zien: over relevante bepalingen uit Richtlijn 95/46 en de Wbp is de ene keer beter nagedacht dan de andere. Dat geldt voor de gevolgen ervan voor de inrichting van de betreffende gegevensverwerkingen in het algemeen, en voor actieve openbaarmaking in het bijzonder. Dat laatste onderwerp staat immers nog niet zo heel lang hoog op de politiek-bestuurlijke agenda. Dit betekent dat er veel verwerkingen zijn van dit type waarbij actieve openbaarmaking niet, onvoldoende of onjuist geregeld is. Voor het kader moet dan worden teruggevallen op het algemene kader van de Wbp

Speciaal relevant zijn in deze context nog de rechten van betrokkenen. Bij wet ingestelde openbare registers vormen namelijk een belangrijke uitzondering op de regel dat betrokkenen zeggenschap hebben over de openbaarmaking van hun persoonsgegevens (zie daarover paragraaf 3.3). De ratio achter openbare registers zoals het Handelsregister of het Kadaster is dat ze bij wet zijn ingesteld om een bepaald publiek belang te dienen. Betrokkenen hebben bij openbare registers geen mogelijkheid om met een beroep op de Wbp verzet aan te tekenen of verwijdering te vragen, ook niet als de registers op internet worden gepubliceerd. De rechten van betrokkenen zijn in het geval van openbare registers afhankelijk van de rechten die de specifieke wet hen toekent.<sup>79</sup> Juist vanwege het ontbreken van een algemene mogelijkheid om bovenmatige of onjuiste gegevens te laten verwijderen is het van groot belang dat de overheid bij het ontsluiten van openbare registers op internet nadrukkelijk onderscheid blijft maken tussen de gegevens die noodzakelijk zijn om een dienst van de overheid te krijgen (zoals een vergunning) en gegevens die op internet worden gepubliceerd.<sup>80</sup>

Let wel: het gaat hier uitsluitend om de situatie waarin bij wet voorzien is in publicatie van gegevens uit een openbaar register op internet. Momenteel geldt voor de meeste openbare registers dat de wet niet voorschrijft dat de gegevens uit het register ook op internet geplaatst worden. Het verantwoordelijke bestuursorgaan kan dan slechts tot publicatie overgaan indien die wijze van openbaarmaking een grondslag vindt in artikel 8 onder e Wbp (zie paragraaf 2.4.2.1). In dat geval kan de betrokkene wél een beroep doen op zijn recht van verzet.

### **Landbouwtelling**

Hieronder wordt de verwerking van persoonsgegevens in het kader van de landbouwtelling behandeld, waaronder de vraag of de gegevens actief openbaar gemaakt zouden kunnen worden. Voor alle duidelijkheid zij benadrukt dat het CBP niet bekend is met voornemens van LNV om over te gaan tot het openbaar maken van de gegevens van de landbouwtelling.

<sup>78</sup> Zie bijvoorbeeld de casus "Landbouwtelling" hieronder.

<sup>79</sup> Artikel 36 vijfde lid Wbp bepaalt dat het recht van correctie en verwijdering niet van toepassing is op bij wet ingestelde openbare registers indien de wet al voorziet in een procedure voor verbetering, aanvulling, verwijdering of afscherming van gegevens. Het recht van verzet uit artikel 40 Wbp is helemaal niet van toepassing op openbare registers die bij wet zijn ingesteld, ongeacht of de wet een bijzondere procedure kent of niet.

<sup>80</sup> Zie ook het kader "Persoonsgegevens niet vogelvrij" in de inleiding.

De Landbouwwet bepaalt in hoofdstuk III dat de minister van LNV van allen die een agrarisch beroep uitoefenen gegevens kan verzamelen over hun bedrijf:

*§ 3. De landbouwtelling*

Artikel 24

1. Onze Minister kan aan degenen, die in de landbouw hun hoofdbestaan of een gedeelte van hun bestaan vinden of plegen te vinden, beschrijvingsbiljetten uitreiken of zenden, bestemd tot het doen van opgave van de landbouwkundige en technische gegevens van hun onderneming.

2. Degene, aan wie een beschrijvingsbiljet is uitgereikt of gezonden, is verplicht de daarin gestelde vragen duidelijk, zonder voorbehoud en naar waarheid te beantwoorden en het aldus ingevulde biljet ondertekend binnen de daartoe door Onze Minister vastgestelde termijn in te leveren.

Artikel 25 bevat vervolgens nadere regels en delegatiebepalingen over de uitvoering van de landbouwtelling.

Dit is een goed voorbeeld van een wettelijke bepaling die overduidelijk tekort schiet op het punt van gegevensbescherming, in het bijzonder de doelformulering. Uit de MVT uit 1957 is echter af te leiden dat daarmee bedoeld is om te voorzien in de behoefte aan (macro)beleidsinformatie. Aan dat (beperkte) doel was destijds bovendien een bijzondere geheimhoudingsplicht gekoppeld.

In een beschikking<sup>81</sup> van de Minister van Landbouw uit 1980 blijkt deze doelstelling al behoorlijk opgerekt:

Doel van de registratie is het kunnen beschikken over informatie in de vorm van op de persoon herleidbare gegevens ten behoeve van het nationale en internationale landbouwbeleid alsmede onderzoek en voorlichting op het gebied van de landbouw.

Met name opmerkelijk is zonder verdere omhaal gesproken wordt van "op de persoons herleidbare gegevens", terwijl onduidelijk is waarom die nodig zouden zijn met het oog op de geformuleerde doelstellingen. Ook zijn aan de oorspronkelijke doelstelling enkele nieuwe doelstellingen toegevoegd.

De vigerende formele doelstelling van de landbouwtelling is te vinden in de melding van het betreffende bestand bij de FG van het Ministerie van LNV:

- \* de inwinning en registratie van gegevens in de agrarische sector tbv statistisch onderzoek en beleid voor het Centraal Bureau voor de Statistiek obv de Landbouwwet
- \* tbv (wetenschappelijk) onderzoek en interne LNV-beleidsvoering
- \* tbv managementdoeleinden, waaronder het samenstellen van rapportages en overzichten

Opnieuw blijkt sprake van een verdere oprekking van de doeleinden van de verzameling. Bovendien worden de gegevens in de huidige praktijk breder gebruikt dan men op basis van bovenstaande doelomschrijving zou mogen verwachten, en zijn er wensen om dit gebruik nog verder te verbreden.

<sup>81</sup> Beschikking bescherming persoonlijke levenssfeer (Registratie artikel 24 Landbouwwet). Deze beschikking is formeel nog geldig, maar het gaat hier volgens de FG van LNV om verouderde regelgeving die op de rol staat om ingetrokken te worden.

Gelet op het bovenstaande kan men vraagtekens plaatsen bij de huidige inrichting en het huidige gebruik van het landbouwtellingsbestand van LNV.<sup>82</sup> Onder deze omstandigheden zou actieve openbaarmaking van dit bestand diverse bruggen te ver zijn. In de eerste plaats dient (ten minste) het doel van deze gegevensverwerking in de wet te worden beschreven. Vervolgens dient het belang van eventuele actieve openbaarmaking van de betreffende gegevens te worden afgewogen tegen het belang van de betrokken agrarische ondernemers bij de bescherming van hun persoonsgegevens.

### *B. Openbaarheid op grond van de Wob*

Artikel 8 Wob bepaalt dat bestuursorganen uit eigen beweging informatie verschaffen over hun beleid, waaronder de voorbereiding en uitvoering ervan, zodra dat in het belang is van een goede en democratische bestuursvoering. De informatie dient te worden verschaft in begrijpelijke vorm, op zodanige wijze, dat belanghebbende en belangstellende burgers zoveel mogelijk worden bereikt. Uit de wetsgeschiedenis blijkt dat artikel 8 een instructienorm is, die geplaatst is in de sleutel van overheidsvoorlichting.<sup>83</sup> Het op grote schaal openbaar maken van persoonsgegevens van burgers kan daartoe in het algemeen niet gerekend worden. Daar komt nog bij dat bij het opstellen van artikel 8 Wob geen rekening is gehouden met grootschalige actieve openbaarmaking op internet – het artikel stamt immers uit ongeveer dezelfde tijd als het World Wide Web, dat zich pas in de jaren nadien tot een belangrijk medium ontwikkelde. Gelet op het zo essentiële verschil tussen passieve en actieve openbaarmaking, en in het bijzonder publicatie op internet<sup>84</sup>, kan artikel 8 Wob daarom in beginsel niet gezien worden als een wettelijke verplichting tot het actief openbaar maken van persoonsgegevens, en al zeker niet tot actieve openbaarmaking van persoonsgegevens op internet.

### **Hergebruik**

Hoewel het strikt genomen niet om actieve openbaarmaking gaat, lijkt het zinvol om tot slot nog kort in te gaan op het door de overheid aan derden beschikbaar stellen van persoonsgegevens met het oog op hergebruik. De hergebruikregeling uit Hoofdstuk V-A Wob bevat geen wettelijke verplichting tot het beschikbaar stellen van gegevens voor hergebruik. Tenzij er sprake is van een andere wettelijke verplichting zal voor het mogelijk maken van hergebruik van persoonsgegevens daarom een beroep moeten worden gedaan op artikel 8 onder e Wbp: noodzakelijk voor de goede vervulling van een publiekrechtelijke taak. Het hergebruik dat van de gegevens gemaakt wordt zal doorgaans neerkomen op een vorm van actieve openbaarmaking door de partij die de gegevens hergebruikt, met als rechtvaardigingsgrond zijn gerechtvaardigd belang (artikel 8 onder f Wbp). Daarbij mag deze nieuwe verantwoordelijke de gegevens in ieder geval niet op ruimere schaal of eenvoudiger beschikbaar maken dan het verstreckende overheidsorgaan is toegestaan. De verantwoordelijkheid daarvoor ligt niet alleen bij de ontvangende partij (die zich uiteraard aan de Wbp moet houden), maar ook bij het verstreckende overheidsorgaan: dat dient in de noodzakelijkheidstoets van artikel 8 onder e Wbp het voorgenomen hergebruik en de waarborgen waarin daarbij voorzien is nadrukkelijk mee te wegen.

---

<sup>82</sup> Zulke vraagtekens zijn inderdaad ook geplaatst door de FG van LNV in zijn jaarverslag over 2005, URL: [http://www.minlnv.nl/cdlpub/servlet/CDLServlet?p\\_file\\_id=13024](http://www.minlnv.nl/cdlpub/servlet/CDLServlet?p_file_id=13024).

<sup>83</sup> Zie hiervoor bijvoorbeeld: E.J. Daalder, *Toegang tot overheidsinformatie: Het grensvlak tussen openbaarheid en vertrouwelijkheid*, proefschrift Universiteit Leiden, Boom Juridische uitgevers, Den Haag, 2005, blz. 151.

<sup>84</sup> Zie hierover de inleiding bij deze Richtsnoeren.

## COLOFON

### CBP Richtsnoeren

#### Actieve openbaarmaking

*Consultatiedocument*

College bescherming persoonsgegevens,  
Den Haag, maart 2008.

© Niets uit deze uitgave mag worden veelelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

Het College bescherming persoonsgegevens houdt onder de Wet bescherming persoonsgegevens toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. De overheid maakt steeds vaker persoonsgegevens actief openbaar. Dit document geeft aan hoe het College actieve openbaarmaking in het algemeen beoordeelt. Daarnaast geven de Richtsnoeren uitleg over de wet, aan de hand van illustraties uit de praktijk. De focus ligt op actieve openbaarmaking via publicatie op internet.

Voor iedereen die persoonsgegevens actief openbaar maakt, is van belang dat duidelijk is of, wanneer en in welke vorm openbaarmaking is toegestaan. De beleidsregels die in deze Richtsnoeren worden uitgewerkt beogen bij te dragen aan deze duidelijkheid. Helderheid over toepasselijke normen bevordert de naleving ervan en past in een efficiënt handhavingsbeleid.

Het definitieve document zal worden gepubliceerd in de Staatscourant.

Postbus 93374  
2509 AJ Den Haag  
E-MAIL [info@cbpweb.nl](mailto:info@cbpweb.nl)

[www.cbpweb.nl](http://www.cbpweb.nl)  
[www.mijnprivacy.nl](http://www.mijnprivacy.nl)