CBP Richtsnoeren

PUBLICATIE VAN PERSOONSGEGEVENS OP INTERNET

Consultatiedocument

OKTOBER 2007

INHOUD

Inleiding *2*

Stroomschema *4*

1 Basisbeginselen van de bescherming van persoonsgegevens op internet *6*

2 Verplichtingen van de verantwoordelijke *16*

3 Rechten van betrokkenen *36*

4 Toepasselijkheid uitzondering journalistieke doeleinden *40*

5 Doorgifte buiten de EU *46*

6 Handhaving en de rol van het CBP *50*

Managementsamenvatting *54*

Management summary *56*

Bijlage *58*

CBP Richtsnoeren

PUBLICATIE VAN PERSOONSGEGEVENS OP INTERNET

Consultatiedocument

INLEIDING

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.

Op internet worden op heel veel manieren persoonsgegevens gepubliceerd. Internet maakt het door zijn aard zeer laagdrempelig om persoonsgegevens te publiceren: via een website, in een discussieforum of in een online dagboek. Mensen kunnen gegevens over zichzelf publiceren of over anderen. Publicaties op internet zijn over het algemeen wereldwijd 24 uur per dag toegankelijk voor een potentieel zeer omvangrijk en divers publiek. Voor mensen van wie de persoonsgegevens op internet staan, kunnen de consequenties groot zijn, bijvoorbeeld als het gaat om onbewezen verdenkingen of intieme details uit het persoonlijke leven. Zelfs als de gegevens op zichzelf juist zijn, kan door de publicatie op internet een onvolledig beeld ontstaan van een persoon, met een negatieve beoordeling tot gevolg.

Daarom stelt de wet grenzen aan de toelaatbaarheid van de publicatie van persoonsgegevens op internet.

Hoofdregel van de Wet bescherming persoonsgegevens (hierna: Wbp) is dat iedereen die persoonsgegevens publiceert zélf verantwoordelijk is voor de naleving van de wet. Particulieren, ondernemingen, organisaties en instellingen die voornemens zijn gegevens over personen op internet te publiceren, dienen dus zelf *voorafgaand* aan de publicatie te beoordelen of dat wel is toegestaan, en zo ja, aan welke voorwaarden zij daarbij moeten voldoen.

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

Deze richtsnoeren behandelen de hoofdlijnen van de beoordeling van een publicatie van persoonsgegevens op internet, onder de geldende privacywetgeving en jurisprudentie[1)]. Publicaties kunnen ook uit anderen hoofde dan privacybescherming onrechtmatig zijn, bijvoorbeeld omdat ze in strijd zijn met de Auteurswet. De handvatten in deze richtsnoeren zijn beperkt tot de toelaatbaarheid van de publicatie onder de geldende privacywetgeving. In deze richtsnoeren wordt dus niet ingegaan op de rechtmatigheid van de publicatie op grond 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 een publicatie. Publicatievormen die niet bij wijze van voorbeeld in deze richtsnoeren zijn opgenomen, kunnen toch in strijd zijn met de Wbp.

Bij de beoordeling van een publicatie 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.

Deze richtsnoeren lopen niet vooruit op rechterlijke oordelen. Rechterlijke uitspraken kunnen naast wetswijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding vormen tot aanvulling of herziening.

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

1) 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.

STROOMSCHEMA

Bent u een natuurlijk persoon, bedrijf of instelling die de verantwoordelijkheid draagt voor een publicatie op internet? (zie I.2, blz 7)

NEE ➤ Deze richtsnoeren zijn niet op u van toepassing. In het hoofdstuk 'rechten van betrokkenen' kunt u lezen wat uw rechten zijn als gegevens over u tegen uw zin op internet worden gepubliceerd.

JA ⮟

Bevat de publicatie gegevens over (levende) natuurlijke personen? (zie I.3 t/m I.6, blz 8)

NEE ➤ De Wbp is alleen van toepassing op gegevens die herleidbaar zijn naar (levende) natuurlijke personen. Deze richtsnoeren zijn niet op uw publicatie van toepassing.

JA ⮟

Betreffen de gegevens strafrechtelijke gegevens, iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging?(Zie I.8, blz 13)

JA ➤ Publicatie op internet is NIET toegestaan, tenzij de betroffen persoon uitdrukkelijke toestemming heeft gegeven, of de betreffende informatie duidelijk zelf openbaar heeft gemaakt. (Zie I.8.1.1 en I.8.1.2, blz 14)

NEE ⮟

Bevatten de gegevens identificatienummers, zoals het BSN? (Zie I.8.3, blz 15)

JA ➤ Publicatie op internet van identificatienummers is NIET toegestaan. (Zie I.8.3, blz 15)

NEE ⮟

Betreft het een publicatie waarbij de toegang effectief is beperkt tot het eigen huishouden, familieleden en/of kennissen, bijvoorbeeld d.m.v. een wachtwoord? (Zie I.7.1, blz 11)

JA ➤ De publicatie valt onder de uitzondering voor persoonlijk/huishoudelijk gebruik, de Wbp is niet van toepassing.

NEE ⮟

Betreft het een publicatie voor uitsluitend journalistieke, literaire of artistieke doeleinden? (Zie I.7.2 en IV, blz 12 en 40)

JA ➤ De Wbp is deels van toepassing.
Van toepassing zijn:
- definities (I.2 t/m I.6, blz 7)
- behoorlijk en zorgvuldig (blz 7)
- doel en verenigbaarheid (II.2 en II.3, blz 17)
- toestemming of noodzaak (II.4, blz 19)
- kwaliteit (II.7, blz 28)
- beveiliging (II.8, blz 30)

NEE ⮟

Heeft u toestemming van de betrokkenen of een aantoonbare noodzaak om persoonsgegevens te publiceren op internet? (Zie II.4, blz 19)

NEE ➤ U mag geen persoonsgegevens publiceren op internet zonder rechtvaardigingsgrond uit artikel 8 Wbp.

JA ⮟

Als uw publicatie gebaseerd is op toestemming, kunt u dan op verzoek persoonsgegevens verwijderen?

NEE ➤ Iedereen heeft het recht om te allen tijde zijn of haar toestemming in te trekken. Na het intrekken van de toestemming is er geen grondslag meer voor de publicatie; de persoonsgegevens moeten verwijderd worden. (Zie II.4.1.1, blz 20)

JA ⮟

Controleer of u aan uw verplichtingen voldoet op het gebied van:
- doel en verenigbaarheid (II.2 en II.3., blz 17)
- de informatieplicht (II.5, blz 24)
- de meldingsplicht (II.6, blz 27)
- kwaliteit (II.7, blz 28)
- beveiliging (II.8, blz 30)
- rechten van betrokkenen (III, blz 36)
- doorgifte buiten de EU (V, blz 46)

BASISBEGINSELEN VAN DE BESCHERMING VAN PERSOONSGEGEVENS OP INTERNET

1 **Inleiding** *7*

2 **Op wie legt de wet verplichtingen? De verantwoordelijke** *7*

3 **Wat is een persoonsgegeven?** *8*
- 3.1 Iedere informatie *8*
- 3.2 Betreffende een persoon *8*
- 3.3 Direct of indirect identificerend *9*

4 **Wanneer is een gegeven géén persoonsgegeven?** *10*

5 **Anonieme of pseudonieme data** *10*

6 **Termijn van de publicatie** *11*

7 **Uitzonderingen op de toepasselijkheid van de Wbp** *11*
- 7.1 Persoonlijk of huishoudelijk gebruik *11*
- 7.2 Journalistieke, artistieke of literaire doeleinden *12*
- 7.3 Historische, statistische of wetenschappelijke doeleinden *12*

8 **Wat is een bijzonder persoonsgegeven?** *13*
- 8.1 Uitzonderingen op het verwerkingsverbod *14*
  - 8.1.1 Uitdrukkelijke toestemming *14*
  - 8.1.1 Zelf openbaar gemaakt *14*
- 8.2 Beeldmateriaal *14*
- 8.3 Identificatienummers *15*

1 Inleiding

Persoonsgegevens op internet moeten op dezelfde zorgvuldige wijze worden verwerkt als in de offlinewereld. De wet is van toepassing op 'de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens' [2], dus op elke publicatie van persoonsgegevens op internet.[3] Iedereen die persoonsgegevens op internet publiceert, ongeacht of dit een privépersoon is, een bedrijf, een instelling of een bestuursorgaan, 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, informatierechten, 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 publicaties op internet. Hieronder volgen de belangrijkste. Tevens worden drie belangrijke uitzonderingen op de toepasselijkheid van de Wbp kort toegelicht: de verwerking van persoonsgegevens voor persoonlijk/huishoudelijk gebruik; de verwerking voor uitsluitend journalistieke, literaire of artistieke doeleinden en het gebruik voor historische, statistische en wetenschappelijke doeleinden.

2 Op wie legt de wet verplichtingen? De verantwoordelijke

Met de term 'verantwoordelijke' wordt degene aangeduid die de verantwoordelijkheid draagt voor de inhoud van een publicatie op internet. Volgens de wet is dit *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.*
De verantwoordelijke kan de houder van een website zijn, de maker van een persoonlijk profiel, maar ook de eigenaar/beheerder van een discussieforum. In een discussieforum, of in een reactiemogelijkheid onder artikelen, kunnen lezers bijdragen leveren waarin persoonsgegevens worden verwerkt.
In beginsel is iedereen die een bijdrage levert zelf verantwoordelijk voor die verwerking van persoonsgegevens, maar de algemene verantwoordelijkheid voor een zorgvuldige gegevensverwerking ligt bij de houder van het forum, omdat die immers het doel en de middelen bepaalt. De houder van de website of het forum, degene die formeel-juridisch de zeggenschap over de verwerking heeft, biedt de gelegenheid tot het publiceren van gegevens en heeft daarom de plicht om zorg te dragen voor een zorgvuldige omgang met persoonsgegevens.[4]

WEBSITE IN DE VERENIGDE STATEN

Een in Nederland gevestigde verantwoordelijke kan ervoor kiezen om technische middelen buiten Nederland aan te wenden voor een publicatie, bijvoorbeeld door gebruik te maken van webhosting[5] in de Verenigde Staten. Hoewel de website niet op Nederlands grondgebied is gevestigd, is de Wbp toch van toepassing. De Wbp is van toepassing op alle in Nederland gevestigde verantwoordelijken.

2) 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.
3) 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 onvergelijkbaar veel sneller en nauwkeuriger kan plaatsvinden dan wanneer dit handmatig zou moeten geschieden, rechtvaardigt een aangescherpt juridisch regime.'
4) 'Iemand die persoonsgegevens heeft vastgelegd en gebruikt, bijvoorbeeld door deze ter raadpleging aan te bieden, ook al zijn deze anoniem door een derde via Internet aangeleverd, is aanspreekbaar op naleving van dit wetsvoorstel en kan zich niet verschuilen achter het adagium 'geen boodschap aan de boodschap'. Zodra opslag met het oog op raadpleging plaatsvindt, bijvoor beeld in de vorm van een 'cache-service', is er sprake van verwerking.' MvT, blz. 60.
5) Webhosting is het (over het algemeen tegen betaling) verhuren van schijfruimte op een internetserver waarop verantwoordelijken internetpagina's kunnen plaatsen. Dergelijke servers kunnen binnen de EU staan, maar ook erbuiten. Het webhostingbedrijf heeft geen zeggenschap over de inhoud van de publicatie.

De aanbieder van internettoegangsdiensten is meestal geen verantwoordelijke, behalve als hij op eigen initiatief en onder eigen redactie informatie aanbiedt, bijvoorbeeld via een webportaal of een nieuwsbrief.

Met de term 'betrokkene' wordt de persoon bedoeld wiens persoonsgegevens worden verwerkt. Op internet lopen de twee rollen nogal eens door elkaar; wie een persoonlijk webdagboek bijhoudt, kan zowel verantwoordelijke als betrokkene zijn.

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 artikel 2 van het Europees Dataverdrag.[6)]
De Europese privacyrichtlijn 95/46/EG (hierna: de Richtlijn) 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.[7)]

De Artikel 29-werkgroep van samenwerkende privacytoezichthouders in de EU heeft in een recente opinie 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'.

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 waardeoordelen als 'Jan is een betrouwbare lener' of 'Jan is een goede medewerker die promotie verdient.' [8)]

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 resultaatelement.

6) Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 1981, Trb. 1988.
7) Memorie van toelichting bij de Wbp, Kamerstukken II, nr 25 892, nr. 3, blz 46.
8) Opinion 4/2007 on the concept of personal data van de Artikel 29-werkgroep, aangenomen op 20 juni 2007, blz 6.

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 de resultaten van een medisch onderzoek betrekking hebben op de patiënt of zoals de gegevens in een klantenbestand van een bedrijf betrekking hebben op de klant.

Ook de aanwezigheid van een doelelement kan er toe 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 bedrijf een bestand bijhoudt met een overzicht van alle inkomende en uitgaande telefoontjes. Dat bestand kan gebruikt worden om medewerkers te beoordelen.

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 een taxibedrijf met behulp van GPS de locaties van zijn taxi's 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 individuele taxichauffeurs te beoordelen.[9)]

3.3 Direct of indirect identificerend

Het bekendste direct identificerende gegeven is de combinatie van voor- en achternaam.
De bekendste indirect identificerende gegevens zijn (e-mail)adres, telefoonnummer, kenteken en de combinatie postcode/huisnummer.[10)] 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.

IP-ADRES

Is een IP-adres, dat wil zeggen het internetnummer waarmee een computer zichzelf op internet kenbaar maakt, een persoonsgegeven? Ja. Een IP-adres is een persoonsgegeven omdat het door een derde – de internetaanbieder – eenvoudig te herleiden valt tot een natuurlijk persoon, de afnemer van het internetabonnement. Dat het IP-adres in sommige gevallen naar een rechtspersoon leidt, in plaats van naar een natuurlijk persoon, doet niet af aan het feit dat het in de meeste gevallen wel degelijk om persoonsgegevens gaat en dat dus de hele verzameling moet worden behandeld conform de uitgangspunten van de Wbp. Ten slotte is van belang dat op basis van het IP-adres beslissingen kunnen worden genomen over de toegang tot bepaalde informatie, zonder dat een dienstverlener op internet überhaupt enige moeite hoeft te doen om zelf persoonsgegevens te verbinden aan een IP-adres. Denk bijvoorbeeld aan onderscheid naar geografische herkomst bij de toegang tot en de presentatie van (delen van) websites[11)]. Ook het registreren en eventueel op internet publiceren van IP-adressen van bezoekers van een website of deelnemers aan een discussieforum valt dus onder het bereik van de Wbp.

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.

9) Opinion 4/2007, blz 9-12.

10) 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); 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) en over postcodes met huisnummers (oa: Registratiekamer 21 juni 1996, 95.O.043).

11) Opinion 4/2007 , blz 14: 'Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense.'

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.

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.

GENEALOGISCHE WEBSITES

Wie geïnteresseerd is in stamboomonderzoek, vindt op internet steeds meer bronnen, zowel gedigitaliseerd archiefmateriaal als onderzoek door (amateur-) genealogen. Omdat de Wbp niet van toepassing is op overleden personen, zijn er vanuit de Wbp weinig bezwaren tegen het publiceren van een stamboom op internet. Toch ontvangt het CBP regelmatig vragen en klachten over stambomen op internet. In het begrijpelijke streven naar volledigheid bevatten veel stambomen informatie over levende personen, zoals hun geboortedatum. In sommige stambomen worden zelfs de ziekten vermeld waaraan mensen zijn overleden. Dergelijke informatie kan betrekking hebben op nabestaanden en dus een persoonsgegeven zijn, als het gaat om erfelijke ziekten waarmee de kinderen kunnen zijn belast. Dat kan het geval zijn bij een moeder die aan hemofilie leed. Omdat deze ziekte is gebonden aan een gen in het X-chromosoom, geeft zij de ziekte in ieder geval door aan zonen. In dit voorbeeld is de Wbp dus wel van toepassing. Wie een stamboom wil publiceren op internet, doet er verstandig aan om zich in eerste instantie te beperken tot gegevens van overledenen en alleen gegevens op te nemen over levende personen als zij daarin ondubbelzinnig hebben toegestemd. De Wbp kent geen principe als 'wie zwijgt, stemt toe' bij het publiceren op internet van persoonsgegevens. De publicist moet reële moeite doen om de (levende) familieleden te bereiken en hen - voorafgaand aan de publicatie op internet van hun persoonsgegevens - vertellen wat hij over hen wil publiceren en met welk doel. Als een familielid geen toestemming geeft voor een dergelijke vermelding, mogen zijn of haar gegevens niet worden gepubliceerd. De publicist kan in de stamboom op internet een verwijzing opnemen als: 'Uit dit huwelijk kwamen drie kinderen voort, onder wie...'

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.[12)] 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.

5 Anonieme of pseudonieme data

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 publiceren van statistische informatie op internet. 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 persoonsge-

12) Registratiekamer, 16 februari 2001, z2000-1172, URL: http://www.cbpweb.nl/documenten/uit_z2000-1172.stm

gevens worden behandeld.[13] Dat kan het geval zijn bij het gebruik van pseudoniemen voor bijdragen aan een discussieforum. Ook als slechts één forumhouder de identiteit kent van de betrokkene, is het pseudoniem daarmee herleidbaar en is het een persoonsgegeven op alle plaatsen waar het pseudoniem wordt gebruikt. Het gebruik van pseudoniemen kan ook op een andere manier tot herleidbaarheid leiden. Veel mensen gebruiken hetzelfde pseudoniem voor al hun activiteiten op internet. Door zoekmachines kunnen persoonlijke details van een betrokkene ongewild worden gekoppeld aan bijdragen die bedoeld waren anoniem te zijn.

6 Termijn van de publicatie

Verantwoordelijken voor publicaties op internet dienen zich rekenschap te geven van de gevolgen van de vaak lange of onbepaalde termijn van een publicatie. Door technische ontwikkelingen kan een gegeven dat op het moment van publicatie geen persoonsgegeven lijkt, later toch herleidbaar worden naar een persoon. Verantwoordelijken kunnen dan vanaf dat moment worden aangesproken op grond van de Wbp.[14] 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.[15]

7 Uitzonderingen op de toepasselijkheid van de Wbp

Er zijn 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.

7.1 Persoonlijk of huishoudelijk gebruik

De eerste uitzondering is de meest absolute. De Wbp is in het geheel niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend persoonlijke of huishoudelijke doeleinden. Dit om te voorkomen dat alledaagse handelingen van privépersonen, zoals het bijhouden van een adresboek, onder de werking van de wet zouden vallen.

De uitzondering voor persoonlijk/huishoudelijk gebruik in de Wbp betreft gebruik voor 'een duidelijk bepaalbare groep van personen'.[16] De uitzondering geldt ook voor gebruik door familieleden of vrienden die niet tot het directe huishouden behoren, mits de toegang daadwerkelijk afgebakend is tot een benoembare groep familieleden, kennissen of vrienden.

Wie bijvoorbeeld een weblog wil bijhouden op internet voor het eigen gezin en zich wil beroepen op de exceptie van persoonlijk of huishoudelijk gebruik, moet passende maatregelen nemen om de toegang daadwerkelijk te beperken tot die beperkte kring. Dat kan bijvoorbeeld door middel van het hanteren van een verplicht wachtwoord, maar ook door de pagina's met persoonsgegevens af te schermen van zoekmachines. Meer over beveiligingsmaatregelen valt te lezen in hoofdstuk 2.7. van deze richtsnoeren.

Zodra de gegevens echter verstrekt worden aan een onbekend aantal personen, hetgeen het geval is bij vrij toegankelijke publicaties op internet, is de Wbp volledig van toepassing.[17] Veel persoonlijke publi-

13) Zie opinie 4/2007 voor meer voorbeelden, blz 18-21.

14) 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'

15) 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, it 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.'

16) MvT blz 70.

17) MvT blz 69: 'Bij de totstandkoming van de richtlijn hebben de Raad van Ministers en de Europese Commissie hierover voor de notulen verklaard dat deze formulering er niet toe mag leiden dat de verwerking van persoonsgegevens door een natuurlijke persoon, waarbij deze gegevens niet worden verstrekt aan één of meer personen, doch aan een onbepaald aantal personen, kan worden uitgesloten van de richtlijn.'

caties die bedoeld zijn voor een beperkte kring belangstellenden, vallen daarom toch onder de Wbp. Het kan gaan om een website ter verwelkoming van een pasgeborene, beelden van vakantieactiviteiten of een weblog met persoonlijk commentaar op de gebeurtenissen van alledag. Als iedere belangstellende de publicatie kan bekijken en de persoonsgegevens niet afgeschermd zijn tegen verdere verwerking door zoekmachines, is de Wbp volledig van toepassing.

7.2 Journalistieke, artistieke of literaire doeleinden

Op gegevensverwerkingen op internet voor uitsluitend journalistieke, artistieke of literaire doeleinden is de Wbp gedeeltelijk van toepassing.[18] Daarbij heeft de wetgever gezocht naar een balans tussen het recht op bescherming van persoonsgegevens en het recht op vrijheid van meningsuiting. In hoofdstuk 4 van deze richtsnoeren wordt deze balans verder toegelicht en wordt uitgewerkt wanneer een publicatie op internet voldoet aan het criterium van 'uitsluitend journalistieke, artistieke of literaire doeleinden'.

7.3 Historische, statistische of wetenschappelijke doeleinden

Ten slotte is er een uitzonderingsgrond op de toepasselijkheid van de Wbp[19] die het mogelijk maakt dat persoonsgegevens die voor een ander doeleinde zijn verzameld, toch voor historische, statistische of wetenschappelijke doeleinden kunnen worden gebruikt.

Verantwoordelijken die persoonsgegevens op internet willen publiceren in het kader van wetenschappelijk, historisch of statistisch onderzoek, dienen de nodige maatregelen te treffen om ervoor te zorgen dat de gegevens alleen ten behoeve van deze specifieke doeleinden worden verwerkt.[20] Dat kunnen technische maatregelen zijn, zoals afscherming van de publicatie door middel van een wachtwoord (zie ook Hoofdstuk II paragraaf 8 over beveiliging), juridische maatregelen, zoals het contractueel vastleggen van het gebruik dat van de gegevens mag worden gemaakt, maar ook organisatorische maatregelen, zoals het inrichten van een procedure om toegangsverzoeken individueel te kunnen beoordelen. Deze uitzondering zal daarom in de praktijk alleen van toepassing zijn op strikt afgeschermde intranetten.

De verantwoordelijke mag dergelijke gegevens ook langer bewaren dan strikt noodzakelijk voor het oorspronkelijke doeleinde, mits opnieuw adequate beschermingsmaatregelen zijn getroffen tegen oneigenlijk gebruik.[21] Ten slotte hoeven instellingen of diensten voor wetenschappelijk onderzoek of statistiek in bepaalde gevallen niet te voldoen aan de informatieplicht en het inzagerecht.[22]

PUBLICEREN VAN INTERNETSTATISTIEKEN

Voor statistische doeleinden houden veel verantwoordelijken statistieken bij over het gebruik van hun website, waaronder bijvoorbeeld IP-adressen en zoektermen. Wie dergelijke statistieken op internet publiceert, kan zich niet vergewissen van het doeleinde waarvoor bezoekers deze gegevens verder verwerken. Om toch openbaar inzicht te geven in het gebruik van de site, kunnen gegevens over bezoekersaantallen en meest gebruikte zoektermen geanonimiseerd worden gepubliceerd. De statistieken mogen wel voor intern gebruik ontsloten worden voor de medewerkers die de toegang beroepshalve nodig hebben.

18) Considerans 17 van de Richtlijn: 'Overwegende dat wat betreft verwerkingen van geluid- en beeldgegevens voor journalistieke, literaire of artistieke doeleinden, met name in de audiovisuele sector, de beginselen van de richtlijn, met een aantal beperkingen overeenkomstig artikel 9 van toepassing zijn.'

19) Bij de behandeling van de Wbp in de Tweede Kamer heeft de minister overigens gepreciseerd dat het niet om een algemene uitzonderingsgrond gaat, maar om 'een sectorale precisering van de verenigbaarheidseis in de vorm van een onweerlegbaar rechtsvermoeden'. Kamerstukken II, nr 25 892, nr. 6, blz. 17.

20) Artikel 9 derde lid Wbp: 'Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden, wordt niet als onverenigbaar beschouwd, indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.'

21) Artikel 10 tweede lid Wbp: 'Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.'

22) Artikel 44 Wbp: 'Indien een verwerking plaatsvindt door instellingen of diensten voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt, kan de verantwoordelijke een mededeling als bedoeld in artikel 34 achterwege laten en weigeren aan een verzoek als bedoeld in artikel 35 te voldoen.'

Het publiceren op internet van een archief met persoonsgegevens, bijvoorbeeld een verzameling historische homepages, ten behoeve van een historisch, statistisch of wetenschappelijk doeleinde , is alleen toegestaan als de verantwoordelijke de nodige maatregelen heeft getroffen om ervoor te zorgen dat de gegevens ook uitsluitend voor dat historisch, statistisch of wetenschappelijk doel worden gebruikt. Als een archief met persoonsgegevens ook *bijzondere* persoonsgegevens (zie hierna, paragraaf 8) bevat, gelden nog strengere regels. De verwerking daarvan is verboden, tenzij een van de uitzonderingen van toepassing is. Twee belangrijke algemene uitzonderingen zijn dat de betrokkene de gegevens duidelijk zelf openbaar heeft gemaakt (bijvoorbeeld in het geval van een homepage en alleen voor zover het gegevens over de betrokkene zelf bevat) of als de betrokkene uitdrukkelijk toestemming heeft gegeven voor publicatie. De Wbp kent daarnaast een specifieke uitzondering op het verwerkingsverbod van bijzondere persoonsgegevens voor wetenschappelijk onderzoek of statistiek (en dus niet voor algemene historische doeleinden!), maar alleen als aan vier voorwaarden is voldaan:

1 Het onderzoek dient een algemeen belang;
2 De verwerking van de bijzondere gegevens is voor het betreffende onderzoek noodzakelijk;
3 Het vragen van uitdrukkelijke toestemming blijkt onmogelijk of kost een onevenredige inspanning;
4 Bij de uitvoering van het onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.[24)]

Een archief van internetpagina's met persoonsgegevens mag dus wel aangelegd worden voor wetenschappelijke doeleinden en via terminals in de bibliotheek ontsloten worden voor een beperkte groep wetenschappers, maar mag niet automatisch opnieuw op internet worden gepubliceerd. Niet iedere wetenschapper mag bovendien automatisch toegang krijgen tot het gedigitaliseerde materiaal; de erfgoedinstelling moet elke specifieke onderzoeksvraag toetsen aan de vier bovengenoemde eisen.

De Juridische Wegwijzer Archieven en Musea online concludeert daarom terecht: *Het verwerken van bijzondere persoonsgegevens in het kader van de digitale beschikbaarstelling van erfgoed kan dus op zeer gespannen voet staan met de Wbp. Beschikbaarstelling van bijzondere persoonsgegevens aan een groot, onbepaald publiek is problematisch; de uitzondering ten behoeve van wetenschappelijk onderzoek levert immers geen soelaas voor de instelling die zijn materiaal breed beschikbaar wil stellen.*[25)]

8 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. Van belang is dat het begrip 'strafrechtelijke gegevens' zowel informatie over veroordelingen omvat 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[26)], tenzij de betrokkene daarvoor uitdrukkelijke toestemming heeft gegeven, of als de betrokkene de gegevens bewust zelf openbaar heeft gemaakt.

23) Publicatie van de zoektermen is overigens risicovol, bleek toen AOL een groot aantal zoekresultaten publiceerde in augustus 2006, nadat de Amerikaanse justitie deze had opgevraagd. De zoektermen bleken ook persoonsgegevens te bevatten, zoals de namen van mensen die naar zichzelf zochten.

24) Artikel 23 tweede lid Wbp.

25) Annemarie Beunen en Tjeerd Schiphof, Juridische Wegwijzer Archieven en Musea online, in opdracht van de Taskforce Archieven en Museumvereniging, 2006, blz. 44.

26) De wettelijke uitzonderingen staan beschreven in de artikelen 17 tot en met 22 Wbp, 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 op de (open) publicatie van persoonsgegevens op internet.

8.1 Uitzonderingen op het verbod om bijzondere persoonsgegevens te publiceren

Wie toch bijzondere persoonsgegevens op internet wil publiceren, kan gebruik maken van een van de twee hierboven al 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.

8.1.1 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.[27)] 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).

8.1.2 Zelf openbaar gemaakt

Iedere volwassene die op zijn of haar eigen homepage of weblog met opzet en onder eigen naam gevoelige informatie over zichzelf publiceert, zoals verslagen van medische perikelen, maakt die gegevens duidelijk zelf openbaar. Daardoor vervalt het verbod om die bijzondere gegevens te verzamelen en te verwerken.
Of iemand een bijzonder gegeven heeft openbaar gemaakt, hangt soms af van de intentie van de betrokkene. Een politicus die zich verkiesbaar stelt, maakt zijn politieke gezindheid duidelijk openbaar. Dat geldt ook voor een imam die in die hoedanigheid in het openbaar uitspraken doet over de Islam. Maar het geldt niet voor een ziekmelding of voor een lichamelijke handicap. Hoewel een lichamelijke handicap vaak voor eenieder zichtbaar is, maakt de betrokkene dit gezondheidsgegeven niet uit vrije wil openbaar. Het gegeven mag dus niet worden verwerkt, tenzij de betrokkene er actief in het openbaar aandacht voor vraagt, bijvoorbeeld als belangenbehartiger van een patiëntenvereniging.

8.2 Beeldmateriaal

Ook foto's, video- en geluidsopnamen van herkenbare natuurlijke personen zijn persoonsgegevens.[28)] Herkenbaar is daarbij breder dan direct identificeerbaar. Zelfs als het gezicht van een betrokkene wordt gemaskeerd, bijvoorbeeld met een zwart balkje, kan een foto een persoonsgegeven zijn. Dat is bijvoorbeeld het geval bij publicatie van camerabeelden van vermeende winkeldieven. Er bestaat een kans dat de betrokkenen herkend worden door hun vrienden, bekenden of buren, op grond van hun uiterlijk, kapsel en kleding.[29)]

Omdat foto's en video's bijzondere persoonsgegevens over ras prijsgeven, stelt de Wbp strikte beperkingen aan het gebruik ervan. De non-discriminatiegrond ras van artikel 1 van de Grondwet omvat ook huidskleur, afkomst en nationale of etnische afstamming.

Als een verantwoordelijke beeldmateriaal over zichzelf publiceert, maakt hij de gegevens duidelijk zelf openbaar (de eerste uitzondering op het verwerkingsverbod van bijzondere persoonsgegevens). Als een verantwoordelijke opnames van andere natuurlijke personen op internet wil publiceren, moet hij daarvoor voorafgaand uitdrukkelijke toestemming hebben gekregen of kunnen aantonen dat de betrokkenen deze foto's of video-opnamen zelf bewust openbaar hebben gemaakt. Alleen ten behoeve van publicaties met uitsluitend journalistieke, artistieke of literaire doeleinden (zie hoofdstuk 4 van deze richtsnoeren) gelden ruimere verwerkingsmogelijkheden van beeld- en geluidsmateriaal. Daarnaast is de Wbp niet van toepassing op publicatie van bijzondere persoonsgegevens op internet voor uitsluitend persoonlijke of huishoudelijke doeleinden. Privépersonen kunnen op grond van die exceptie dus bijvoorbeeld vrijelijk familiefoto's op internet publiceren, mits de toegang adequaat is afgeba-

27) MvT, blz 122-123.
28) 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.'
29) Opinion 4/2007, Example No. 19: Publication of video surveillance, blz 21.

8.3 kend tot een duidelijk bepaalbare groep van personen.

Identificatienummers

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 sofinummer (straks: burgerservicenummer) op internet te publiceren, zelfs niet als de betrokkene er toestemming voor heeft gegeven.

II

VERPLICHTINGEN VAN DE VERANTWOORDELIJKE

1 **Inleiding** *17*

VOORAFGAAND AAN PUBLICATIE

2 **Legitieme doeleinden** *17*

3 **Verdere verwerking** *17*
- 3.1 Hergebruik van persoonsgegevens uit andere publicaties *18*
- 3.2 Hergebruik van persoonsgegevens door derden *18*
- 3.3 Geheimhoudingsplicht *19*

4 **Toestemming vragen of noodzaak kunnen aantonen** *19*
- 4.1 Toestemming *20*
  - 4.1.1 Toestemming intrekken *20*
  - 4.1.2 Toestemming van personen onder de zestien jaar *21*
- 4.2 Noodzaak *21*
  - 4.2.1 Uitvoering van een overeenkomst *21*
  - 4.2.2 Wettelijke verplichting *22*
  - 4.2.3 Vitaal belang *22*
  - 4.2.4 Goede vervulling publiekrechtelijke taak *22*
  - 4.2.5 Gerechtvaardigd belang *22*

BIJ PUBLICATIE

5 **Informatieplicht** *24*
- 5.1 Omvang informatieplicht *24*
- 5.2 Informatieplicht jegens inwoners buiten de EU *25*
- 5.3 Privacyverklaring *25*
- 5.4 Identiteitsvermelding *26*

6 **Meldingsplicht** *27*
- 6.1 Wat betekent een melding? *27*
- 6.2 Vrijstellingsbesluit *27*
- 6.3 Toekomst: uitbreiding vrijstellingen internetpublicaties *27*

7 **Kwaliteit** *28*
- 7.1 Beperkt bewaren *28*
- 7.2 Toereikend, ter zake dienend en niet bovenmatig *28*
- 7.3 Juist en nauwkeurig *29*
- 7.4 Identiteitsvaststelling alleen elektronisch? *29*
- 7.5 Gebruik identiteitsbewijs *30*

8 **Beveiliging** *30*
- 8.1 Passende beveiligingsmaatregelen *30*
- 8.2 Tegengaan onnodige publicatie persoonsgegevens *31*
- 8.3 Afscherming persoonsgegevens van zoekmachines *31*
- 8.4 Gebruik van wachtwoorden of andere doelgroepafbakening *32*
  - 8.4.1 Dictionary attacks *33*
- 8.5 Beveiliging gegevenstransport *33*
- 8.6 Beveiliging machines tegen onbevoegde toegang *33*

NA PUBLICATIE

9 **Verwijderen onrechtmatigheden** *36*
- 9.1 Plicht tot verwijderen onjuiste gegevens *51*

1 Inleiding

Onrechtmatige publicaties van persoonsgegevens moeten door de verantwoordelijke onmiddellijk van internet worden verwijderd. Maar ook voorafgaand aan de publicatie van persoonsgegevens op internet dient een verantwoordelijke 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 publicatie vast te stellen of de publicatie een legitiem doeleinde dient en of dat doel verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verkregen. De verantwoordelijke dient bij voorkeur toestemming te vragen van de betrokkenen, of anders te kunnen onderbouwen dat publicatie is toegestaan op grond van een van de andere wettelijke regels over de noodzakelijkheid van de publicatie.

Bij de publicatie dienen verantwoordelijken betrokkenen actief te informeren over het doel en de opzet van de publicatie. 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 de gepubliceerde 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 publicatie nog wijzigingen aan te brengen, bijvoorbeeld als een betrokkene zijn toestemming voor publicatie intrekt, of als de gegevens onrechtmatig blijken te zijn.

VOORAFGAAND AAN PUBLICATIE

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 doeleinde kan bijvoorbeeld zijn: voortzetting van het papieren clubblad op internet, met als doeleinde het informeren van de leden van de vereniging over de verenigingsactiviteiten. Een doeleinde mag niet zo vaag of ruim zijn dat er geen kader is om te toetsen of de gegevens werkelijk nodig zijn voor het gestelde doel.

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.

GEGEVENS VAN OUD-LEERLINGEN

Een school voor voortgezet onderwijs vraagt alle leerlingen of ze ook na het eindexamen hun correcte contactgegevens willen blijven doorgeven aan de schooladministratie, zoals adres, telefoonnummer en e-mailadres. De school noemt het organiseren van toekomstige reünies als doeleinde, evenals het kunnen toesturen van andere informatie over lustra en jubilea van de school. De school wordt regelmatig benaderd door oud-leerlingen die contact zoeken met voormalige klasgenoten. De school besluit de contactgegevens van alle oud-leerlingen op internet te publiceren, om hen in staat te stellen makkelijker zelf contact met elkaar op te kunnen nemen. Deze werkwijze is in strijd met het doelbindingsprincipe uit de Wbp, omdat de gegevens voor een ander doeleinde zijn verzameld en de publicatie op internet vervelende gevolgen kan hebben voor de betrokkenen. De publicatie op internet van de contactgegevens kan bijvoorbeeld leiden tot spam of ongewenst contact met andere oud-leerlingen, maar ook in algemene zin tot een oordeel door derden over iemands kwaliteiten in relatie tot de kwaliteit en aard van de betreffende school. Als de school de oud-leerlingen in staat wil stellen contact met elkaar op te nemen, moet ze een andere manier kiezen, bijvoorbeeld op basis van expliciete toestemming bij het verzamelen van de gegevens. Daarbij is het belangrijk dat de school nadenkt over passende waarborgen, zoals afscherming van de gegevens door middel van een (uniek) wachtwoord en afscherming van de pagina's voor zoekmachines.

3.1 Hergebruik van persoonsgegevens uit andere publicaties

Veel mensen gebruiken gegevens van andere websites voor een eigen publicatie, zoals foto's waar mensen herkenbaar op staan of adressen. De Wbp stelt echter belangrijke beperkingen aan het hergebruik. Het feit dat persoonsgegevens op internet staan, betekent niet dat ze zomaar opnieuw gebruikt mogen worden in een andere context, voor een ander doeleinde. Het nieuwe doel moet verenigbaar zijn met het oude doel en de verantwoordelijke dient een zelfstandige rechtvaardigingsgrond te hebben voor de publicatie. Iemand die bijvoorbeeld een weblog bijhoudt waarin hij of zij ook bijzondere persoonsgegevens over zichzelf verwerkt, zoals een beschrijving van gezondheidsklachten, maakt die gegevens zelf openbaar. Hergebruik van bijzondere persoonsgegevens is niet verboden als de betrokkene de gegevens zelf openbaar heeft gemaakt, maar de verantwoordelijke die deze gegevens in een eigen publicatie wil verwerken, dient een zelfstandige rechtvaardigingsgrond te hebben (zie hierna paragraaf 4: toestemming vragen of noodzaak aantonen).

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 overnemen van verouderde, onjuiste informatie over iemands functie of beroep. De onderwerpen kwaliteit en beveiliging komen nader aan de orde in de paragrafen 7 en 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.

3.2 Hergebruik van persoonsgegevens door derden

Verantwoordelijken dienen zich bij het beoordelen of (her-)publicatie van persoonsgegevens op internet verenigbaar is met het oorspronkelijke doeleinde niet alleen rekenschap te geven van de herkomst van de gegevens, maar ook van het risico dat anderen de gegevens gebruiken die de verantwoordelijke zelf op internet publiceert. Om de risico's voor betrokkenen te verkleinen, dient elke verantwoordelijke adequate beveiligingsmaatregelen te treffen tegen oneigenlijk verder gebruik.

Voor een juiste risico-inschatting moet de rol van zoekmachines worden meegewogen. Publicaties op internet die eigenlijk gericht zijn op een klein publiek, worden door zoekmachines wereldwijd toegankelijk gemaakt. Zoekmachines kunnen verspreide informatie van verschillende aard over een persoon koppelen. Dat kan een nieuw beeld opleveren, met een veel hoger risico voor de betrokkene dan elk van de afzonderlijke gegevens meebrengt. 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 8 van dit hoofdstuk.

OMGEKEERD ZOEKEN NAAR NUMMERS

Naast de algemene privacyrichtlijn uit 1995 hebben het Europees Parlement en de Raad van de Europese Unie in 2002 een bijzondere richtlijn aangenomen ter bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.[30)] Deze richtlijn is in Nederland omgezet in hoofdstuk 11 van de Telecommunicatiewet (Tw), over de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Artikel 11.6 Tw bevat bepalingen over het gebruik van abonneegegevens in openbare lijsten. De reikwijdte van dit artikel is strikt genomen weliswaar beperkt tot partijen die een directe relatie met de betrokkene onderhouden, zoals een telefoonmaatschappij of een bedrijf dat door een telefoonmaatschappij is ingehuurd met het doel om een abonneelijst uit te geven, maar de bepalingen geven een nadere invulling aan de algemene bepalingen uit de Wbp over verenigbaar gebruik.

Volgens de Tw mogen aanbieders van telecommunicatiediensten openbare abonneelijsten uitgeven en die desgewenst op internet publiceren. De gegevens van betrokkenen (natuurlijke personen) mogen daarin echter alleen worden opgenomen als zij daarin toestemmen. Bovendien heeft iedereen het recht om zijn persoonsgegevens in dergelijke lijsten kosteloos te laten verbeteren of te laten verwijderen. Als het gaat om elektronische publicaties moeten de aanbieders van de lijsten duidelijk maken wat de gebruiksmogelijkheden zijn op basis van daarin opgenomen zoekfuncties. Artikel 11.6 derde lid Telecommunicatiewet (Tw) voegt daar aan toe dat voor elk ander doeleinde dan het zoeken van een nummer aan de hand van een naam in combinatie met het adres, inclusief huisnummer, postcode en woonplaats, afzonderlijke toestemming van de abonnee vereist is. Wie een dienst wil aanbieden om op internet omgekeerd te zoeken, aan de hand van een nummer naar de naam en het adres van een abonnee, heeft dus afzonderlijke toestemming nodig van elk van de betrokkenen. Als het gaat om verantwoordelijken die geen relatie hebben met de abonnee, is volgens de Wbp het doeleinde van belang waarvoor de gegevens zijn verzameld. Bij abonneelijsten is het doel om nummers op te zoeken die behoren bij personen, om gebruik te kunnen maken van een elektronische communicatiedienst. Omgekeerd zoeken dient andere doeleinden, zoals het volgen van personen of gebruik voor directmarketingdoeleinden, en is daarom, ook vanwege de risico's voor betrokkenen, niet verenigbaar met het oorspronkelijke doeleinde.

3.3 Geheimhoudingsplicht

De Wbp verbiedt publicatie van persoonsgegevens indien de gegevens onder een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift vallen.[31)] 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 VAN 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[32)]: 'Gelet op het vorengaande 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.'

4 Toestemming vragen of noodzaak kunnen aantonen

Voor verantwoordelijken die persoonsgegevens op internet willen publiceren, geldt dat zij toestemming nodig hebben van de betrokkenen, tenzij er een aantoonbare andere noodzaak is voor de publicatie, zoals nakoming van een wettelijke verplichting of uitvoering van een contractuele verplichting. De Wbp noemt dit een grondslag voor een gerechtvaardigde gegevensverwerking. In deze richtsnoeren wordt hiervoor het begrip 'rechtvaardigingsgrond' gehanteerd. Artikel 8 Wbp somt in totaal zes rechtvaardigingsgronden op..[33)] Indien er geen toestemming is (artikel 8 onder a Wbp) mag publicatie uit-

30 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PB L 201/37.

31) Wbp, artikel 9 lid 4.

32) CBP, z2003-01563, 11 februari 2004, URL: http://www.cbpweb.nl/documenten/adv_z2003-1563.stm

33) Zie voor een algemene toelichting op artikel 8 Wbp het informatieblad 'Verstrekken van persoonsgegevens' voor verantwoordelijken, en het informatieblad 'Verstrekken van uw persoonsgegevens' voor betrokkenen, beschikbaar via de website van het CBP, URL: http://www.cbpweb.nl, onder 'nieuws en publicaties', 'publicaties', 'informatiebladen'.

sluitend indien deze noodzakelijk is volgens een van de volgende vijf rechtvaardigingsgronden:
- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst (artikel 8 onder b Wbp);
- om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is (artikel 8 onder c Wbp);
- ter vrijwaring van een vitaal belang van de betrokkene (artikel 8 onder d Wbp);
- voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, (artikel 8 onder e Wbp);
- voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van 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 (artikel 8 onder f Wbp).

Elk van de rechtvaardigingsgronden wordt hierna uitvoerig toegelicht.
Ten aanzien van bijzondere persoonsgegevens, zoals strafrechtelijke gegevens, gelden extra regels. Verwerking ervan is verboden, tenzij de betrokkene de gegevens duidelijk zelf openbaar heeft gemaakt of uitdrukkelijke toestemming heeft gegeven voor de verwerking (zie hoofdstuk I, paragraaf 8).
Opheffing van het verwerkingsverbod ontslaat de verantwoordelijke niet van de plicht om een zelfstandige rechtvaardigingsgrond voor de publicatie te hebben.

4.1 Toestemming

Toestemming, de rechtvaardigingsgrond voor veel publicaties op internet, 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 òf de betrokkene toestemming heeft gegeven en voor welke specifieke verwerkingen hij toestemming heeft gekregen. Als het gaat om een openbaar toegankelijk discussieforum of gastenboek op internet, hoeft de verantwoordelijke echter niet expliciet toestemming te vragen voor publicatie van een reactie; hij mag er redelijkerwijs van uitgaan dat de betrokkene begrijpt dat de reactie op internet verschijnt..[34)]

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. [35)]

4.1.1 Toestemming intrekken

Een eenmaal gegeven toestemming tot het verwerken van gegevens kan te allen tijde worden ingetrokken.[36)] De memorie van toelichting bij de Wbp voegt daar volledigheidshalve aan toe dat een dergelijke intrekking geen consequenties heeft voor gegevensverwerkingen die vóór het moment van de intrekking hebben plaatsgevonden.[37)] Deze inperking heeft echter geen betrekking op het voortduren van de publicatie van persoonsgegevens op internet. Als de toestemming wordt ingetrokken, is de publicatie vanaf dat moment onrechtmatig, tenzij de verantwoordelijke de verwerking kan rechtvaardigen onder een andere rechtvaardigingsgrond. Dat betekent dat verantwoordelijken voor publicaties op internet, voorzover die gebaseerd zijn op toestemming, technische voorzieningen moeten tref-

34) '...) kennis die hij op grond van maatschappelijke opvattingen redelijkerwijs bij de betrokkene aanwezig mag achten.' MvT, blz 66.
35) CBP, april 2004, z2003-1437, URL: http://www.cbpweb.nl/documenten/uit_z2003-1437.stm
36) Artikel 5 Wbp tweede lid: 'Een toestemming kan door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken.'
37) Een eenmaal gegeven toestemming tot het verzamelen van gegevens kan te allen tijde worden ingetrokken. Een dergelijke intrekking heeft echter geen consequenties voor gegevensverwerkingen die vóór het moment van de intrekking hebben plaatsgevonden. Dit geldt voor alle soorten van verwerkingen. Gezien het dwingende karakter van dit voorschrift is dit expliciet bepaald in artikel 5, tweede lid. MvT, blz. 67/68.

fen om persoonsgegevens ook daadwerkelijk te kunnen verwijderen als een betrokkene zijn of haar toestemming intrekt.

4.1.2 Toestemming van personen onder de zestien jaar

Met betrekking tot personen onder de zestien jaar stelt de Wbp bijzondere regels. Voor de verwerking van persoonsgegevens van jongeren onder de zestien jaar kunnen alleen de ouders of wettelijk vertegenwoordiger(s) toestemming geven. De verantwoordelijke moet aan kunnen tonen dat hij toestemming heeft gekregen van de ouders. Als dat niet het geval is, is de toestemming van de betreffende jongere nietig en de publicatie op internet van de persoonsgegevens onrechtmatig.[38)]

De dagelijkse gang van zaken op internet is dat veel jongeren gedetailleerde informatie over zichzelf en hun vrienden en kennissen publiceren op internet, op een eigen website of in sociale netwerkomgevingen. Zo lang de betrokkenen geen hinder ondervinden van dergelijke publicaties, kan het wettelijk toestemmingsvereiste daarbij soms zinloos lijken. Bij publicatie op internet moet echter rekening worden gehouden met het feit dat de gevolgen pas jaren later merkbaar kunnen worden, door koppeling van gegevens over een persoon door de tijd heen, of omdat een jongere zich in een nieuwe omgeving (bijvoorbeeld bij wisseling van school) op een andere manier wil kunnen ontwikkelen dan voorheen.

De grens van 16 jaar in de Wbp betekent dat houders van websites of netwerkomgevingen die speciaal zijn gericht op jongeren onder de 16 jaar een maatschappelijke verantwoordelijkheid hebben om hen te wijzen op hun rechten en plichten, op een heldere en voor de doelgroep begrijpelijke wijze.

Verantwoordelijken voor publicaties of netwerkomgevingen die veel door jongeren worden bezocht, dienen zich om aan de Wbp voldoen in ieder geval aan de volgende regels te houden:

1 Benadrukken dat de gebruikers hun ouders dienen te informeren en om hun toestemming dienen te vragen;
2 Waarschuwen dat gebruikers niet zonder toestemming persoonsgegevens van anderen (veelal zelf ook weer minderjarigen) mogen publiceren;
3 Technische maatregelen doorvoeren om verdere verwerking op internet zoveel mogelijk in te perken, zoals automatische blokkade van persoonlijke profielpagina's voor zoekmachines en persoonlijke controle van de gebruiker over de toegang tot zijn gegevens voor andere gebruikers van de site of omgeving;
4 Strikte inperking van de soorten gegevens die aan jongeren worden gevraagd. Het publiceren van bijzondere persoonsgegevens van minderjarigen, zoals gegevens over seksuele geaardheid of religieuze overtuiging dient altijd achterwege te blijven. Verantwoordelijken mogen er niet vanuit gaan dat jongeren de risico's kunnen doorgronden van beoordeling op grond van een dergelijk kenmerk.

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.

4.2.1 Uitvoering van een overeenkomst

De rechtvaardigingsgrond dat publicatie op internet noodzakelijk is ter uitvoering van een overeenkomst kan van pas komen bij specifieke dienstverlening om via internet te bemiddelen. Dat kan gaan om bemiddeling tussen werkzoekenden en werkgevers, of tussen mensen die op zoek zijn naar contact of een relatie. Daarbij is het wel van belang, in het licht van de informatieplicht uit de Wbp (zie hierna, paragraaf 5) en de bepalingen in het Burgerlijk Wetboek over de toegankelijkheid, begrijpelijk-

38) Artikel 3:40 eerste lid Burgerlijk Wetboek bepaalt dat een rechtshandeling die door inhoud of strekking in strijd is met de goede zeden of de openbare orde, nietig is. De toestemming die met betrekking tot een bepaalde gegevensverwerking niet rechtsgeldig is gegeven, dient als nietig te worden beschouwd. MvT, blz. 67.

39) In navolging van diverse EU richtlijnen is de informatieplicht naar consumenten in de jaren negentig van de 20ste eeuw aangescherpt. In Nederland zijn de verscherpte bepalingen uitgewerkt in de artikelen 233 en 234 Boek 6 BW, over de ter hand stelling van algemene voorwaarden en in de artikelen 236 en 237 Boek 6 BW, over onredelijke bedingen.

heid, redelijkheid en billijkheid van contractuele bepalingen, dat betrokkenen goed worden geïnformeerd over welke gegevens op internet worden gepubliceerd en over de mate waarin de gegevens zijn afgeschermd tegen onbedoeld hergebruik door derden, bijvoorbeeld door een wachtwoord en afscherming van de persoonsgegevens van zoekmachines.[39)]

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. 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. Het CBP zet zich daarbij in voor een duidelijk onderscheid tussen openbaarmaking en publicatie op internet. Het openbaar mogen, of zelfs moeten maken van persoonsgegevens betekent niet automatisch dat de gegevens op internet mogen worden gepubliceerd.

Het onderscheid tussen een wettelijke plicht om bepaalde persoonsgegevens te verzamelen en de publicatie ervan op internet speelde een belangrijke rol in het onderzoek dat het CBP in 2005 deed naar de publicatie op internet van (aanvragen voor) bouwvergunningen door de gemeente Nijmegen. Op het gemeentelijk aanvraagformulier moeten allerlei persoonsgegevens worden ingevuld, zoals naam, adres, e-mailadres, telefoonnummer, handtekening en hoogte van de bouwsom. De gemeente scande de aanvraagformulieren in en publiceerde die op internet. Het CBP stelde vast dat er wel een wettelijke verplichting was tot het bijhouden van een bouwregister, maar geen wettelijke verplichting om alle documenten integraal op internet te publiceren.

Het CBP schreef: *Dit rechtvaardigt niet zonder meer dat alle persoonsgegevens waarvan de gemeente gebruik heeft gemaakt in de procedure voor het verlenen van de bouwvergunning - gegevens die op goede gronden in het bouwregister voorkomen - opgenomen worden in het via internet toegankelijke Digitaal Bouwarchief. Dat de gemeente bepaalde persoonsgegevens noodzakelijkerwijs mag opnemen (in het analoge archief, red.), betekent namelijk op zich niet dat de gemeente die gegevens ook, al dan niet beperkt, aan anderen ter beschikking mag stellen.*[40)]

4.2.3 Vitaal belang

De rechtvaardigingsgrond dat publicatie noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene heeft betrekking op een medische noodzaak. Het artikel is bedoeld om mensenlevens te kunnen redden in acute noodsituaties, als de betrokkene bijvoorbeeld buiten bewustzijn is. Het is hoogst onwaarschijnlijk dat deze rechtvaardigingsgrond gebruikt kan worden om een publicatie op internet te rechtvaardigen.

4.2.4 Goede vervulling publiekrechtelijke taak

Overheidsinstellingen of -diensten die persoonsgegevens op internet willen publiceren, kunnen een rechtvaardigingsgrond vinden in artikel 8 onder e Wbp. Er is een rechtvaardigingsgrond als publicatie noodzakelijk is voor een goede vervulling van een publiekrechtelijke taak van het desbetreffende bestuursorgaan. Daarbij moet voor elk te publiceren gegeven de noodzaak zorgvuldig worden afgewogen. Dat verstrekking van bepaalde gegevens aan een bestuursorgaan noodzakelijk is, rechtvaardigt niet dat alle gegevens automatisch ook op internet worden gepubliceerd. Dat geldt ook voor bestuursorganen die actieve openbaarmaking overwegen in het kader van de Wet openbaarheid van bestuur (Wob).[41)]

4.2.5 Gerechtvaardigd belang

Een laatste rechtvaardigingsgrond zit in de afweging van het eigen gerechtvaardige publicatiebelang tegen de rechten en vrijheden van betrokkenen, in het bijzonder de bescherming van hun persoonlijke levenssfeer. De afweging is veel algemener van aard dan de eerste vijf rechtvaardigingsgronden en is naar zijn aard afhankelijk van de omstandigheden van een specifieke publicatie. In beginsel zullen slechts weinig publicaties zich op deze rechtvaardigingsgrond kunnen beroepen, omdat publicatie op internet onvoorspelbare risico's met zich meebrengt voor de persoonlijke levenssfeer van betrokkenen.

40) CBP, z2005-0212, 1 december 2005, URL: http://www.cbpweb.nl/documenten/uit_z2005-0212.shtml

41) Met het oog op de privacyaspecten van actieve openbaarmaking zal het CBP binnen afzienbare tijd beleidsregels publiceren over de verhouding Wob - Wbp.

Een verantwoordelijke die zich op artikel 8 onder f Wbp wil beroepen moet allereerst aantonen dat een voorgenomen publicatie noodzakelijk is voor de verwezenlijking van een gerechtvaardigd eigenbelang. Noodzaak is volgens jurisprudentie van het EHRM niet hetzelfde als 'leuk' of 'nuttig'.[42] Bovendien dient de verantwoordelijke aan te tonen dat het beoogde belang niet anderszins of met minder ingrijpende middelen kan worden gediend[43].

Nadat deze afweging is gemaakt, dient de verantwoordelijke een tweede afweging te maken, waarbij de individuele belangen van betrokkenen een zelfstandig gewicht in de schaal leggen. Een verantwoordelijke kan niet volstaan met de redenering dat het om gegevens gaat die toch al op andere plaatsen op internet zijn te vinden en dat de inbreuk van de nieuwe publicatie daarom gering zou zijn.

De memorie van toelichting bij de Wbp geeft als hulpmiddel vier vragen die verantwoordelijken kunnen stellen om de dubbele afweging te maken.
- Is er werkelijk een belang dat verwerking van persoonsgegeven rechtvaardigt?
- Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan – afhankelijk van de ernst van de inbreuk – gegevensverwerking niet achterwege te blijven?
- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg – zonder verwerking – worden bereikt?
- Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel? [44]

Dit komt er op neer dat de verantwoordelijke zich moet afvragen:
– Is publicatie echt nodig? Kan het niet anders?
– Weegt deze publicatie wel op tegen het daarmee nagestreefde doel?
– Wat betekent publicatie voor elke individuele betrokkene in zijn specifieke geval?

Een verantwoordelijke dient het resultaat van deze afweging inzichtelijk te kunnen maken. Het resultaat van de afweging moet een duidelijk belang zijn, dat maatschappelijk aanvaardbaar is, niet in strijd met wat volgens geschreven en ongeschreven recht in het maatschappelijk verkeer betaamt. De verantwoordelijke mag het belang van de verwerking niet snel laten prevaleren boven het belang van de betrokkene, juist ook vanwege de risico's van verdere verwerking door publicatie op internet.

Dat het belang van betrokkenen zwaar weegt en vaak prevaleert boven het belang van de verwerking, blijkt ook uit jurisprudentie over het publiek etaleren van foto's van vermeende winkeldieven. In augustus 2004 oordeelde de voorzieningenrechter van de rechtbank Amsterdam[45] dat een winkelier geen foto in zijn winkel mocht ophangen van een vrouw die hij aanzag voor een winkeldief. De publicatie zou in strijd zijn met de auteurswet, maar ook met de Wbp, in het bijzonder met artikel 8 onder f. *Het ophangen van de foto van [eiseres] met daarbij de tekst 'Deze vrouw heeft hier gestolen' is eveneens in strijd met de Wbp. De videobeelden gemaakt met een bewakingscamera zijn aan te merken als een bestand in de zin van artikel 1 onder c van de Wbp, nu sprake is van een gestructureerd geheel van persoonsgegevens. De verwerking van deze gegevens door een winkelier valt onder de Wbp. Uit hetgeen hiervoor (….) is overwogen, volgt dat [eiseres] geen ondubbelzinnige toestemming heeft gegeven voor de verwerking van de videobeelden tot een foto - zoals vereist in artikel 8 onder a Wbp - en dat het belang van [eiseres] prevaleert bij de in artikel 8 onder f Wbp bedoelde belangenafweging.*[46]

De rechter in kort geding overwoog daarbij (in punt 9) : *"Een publicatie als de onderhavige - die een element van straf in zich heeft - levert eigenrichting op jegens [eiseres]."* En voegde er aan toe: *"Het opsporen en berechten van verdachten is het monopolie van justitie en het is niet aan burgers om mogelijke verdachten openlijk te schande te zetten."*

42) EHRM 25 maart 1983, Silver and others v. United Kingdom, nr. 97: '(a) the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable […].'

43) Een dergelijke afweging van belangen moet volgens vaste jurisprudentie van het EHRM in overeenstemming zijn met de beginselen van proportionaliteit en subsidiariteit. Dit laatste betekent dat de inbreuk op de persoonlijke levenssfeer van de betrokkene in een juiste verhouding moet staan tot het nagestreefde doel en dat dit niet op een minder ingrijpende wijze kan worden bereikt.

44) MvT, blz. 86.

45) LJN: AQ7877, Rechtbank Amsterdam, KG 04/1566 SR

46) Idem, onder punt 12.

Twee jaar later, nadat de gewraakte foto opnieuw was gepubliceerd in een dagblad, deed het CBP een algemene uitspraak over de toelaatbaarheid van publicaties van foto's van verdachten van winkeldiefstal door particuliere ondernemingen.[47] Het CBP oordeelde dat de Wet bescherming persoonsgegevens niet toelaat dat foto's van personen die verdacht worden van winkeldiefstal door winkeliers op winkelruiten of andere voor het publiek zichtbare plaatsen worden gepubliceerd.

Geoordeeld is: *Het gebruik van de beelden voor publicatie in winkels, zodat er feitelijk sprake is van het publiekelijk betichten van strafbare feiten (shaming), kan niet gerekend worden tot een maatschappelijk aanvaardbaar doel. Daarmee is gegeven dat het eveneens geen gerechtvaardigd belang kan zijn voor de verantwoordelijke.*[48]

BIJ PUBLICATIE

5 Informatieplicht

De Wbp bevat een informatieplicht. Verantwoordelijken voor publicaties op internet moeten op eigen initiatief inzicht geven in het doel van de publicatie, hoe en welke persoonsgegevens ze verwerken 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 zelf verzamelen (artikel 33 Wbp), maar ook als zij de gegevens op een andere manier verkrijgen, bijvoorbeeld door gegevens over te nemen uit andere publicaties op internet (artikel 34 Wbp). Wie gegevens op internet verzamelt en voor een eigen publicatie wil hergebruiken, moet de betrokkenen individueel op de hoogte stellen dat er een nieuwe verantwoordelijke is die de persoonsgegevens verwerkt.[49] Als er weinig risico's gemoeid zijn met de publicatie 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.

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.[50] 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, zeker als niet op voorhand duidelijk is dat de gegevens ook op internet worden gepubliceerd en hen te wijzen op hun recht op verzet. 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 onmogelijkheden – 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, bijvoorbeeld van welke andere internetpublicaties hij de gegevens heeft overgenomen.

47) CBP, 30 mei 2006, z2005-0846, URL: http://www.cbpweb.nl/documenten/uit_z2005-0846.shtml
48) CBP, 30 mei 2006, z2005-0846, blz 3.
49) Zie voor een algemene toelichting op de informatieplicht het informatieblad 'Informatieplicht' voor verantwoordelijken, beschikbaar via de website van het CBP, URL: http://www.cbpweb.nl, onder 'nieuws en publicaties', 'publicaties', 'informatiebladen'.
50) MvT, blz. 149-150.

SCHRIJVEN OVER BEKENDE PERSONEN

Een minister vertelt op televisie over zijn privéleven. Tal van persoonlijke, niet-journalistieke weblogs besteden aandacht aan zijn uitspraken en allerlei mensen geven daar weer commentaar op. In dit geval, omdat de bewindsman zijn uitlatingen in het openbaar heeft gedaan, mag aangenomen worden dat hij op de hoogte is van het feit dat hierover in het openbaar verder wordt gediscussieerd, ook op internet. De houders van de weblogs hoeven de minister daarom niet apart te informeren dat ze persoonsgegevens over hem verwerken. Een (niet-journalistieke) verantwoordelijke die de aanleiding echter te baat neemt om allerlei andere privé-informatie over de minister op internet te publiceren, inclusief bijvoorbeeld foto's van zijn familie, dient de minister wel degelijk te informeren. Of een dergelijke publicatie überhaupt te rechtvaardigen valt, is zeer de vraag, gezien de mogelijke gevolgen voor de familieleden.

5.2 Informatieplicht jegens inwoners buiten de EU

De informatieplicht geldt jegens alle betrokkenen over wie persoonsgegevens worden verwerkt, ook als het gaat om inwoners uit een land buiten de Europese Unie. Als een verantwoordelijke bijvoorbeeld een contactlijst wil publiceren van mensen uit de hele wereld met een hele specifieke interesse, dan moeten alle betrokkenen voorafgaand aan de publicatie individueel op de hoogte worden gesteld. Als een inwoner uit de Verenigde Staten merkt dat zijn naam op de desbetreffende website staat zonder dat hij daarover tevoren is geïnformeerd, kan hij in Nederland de rechtsmiddelen aanwenden die de Wbp hem toekent.[51)]

5.3 Privacyverklaring

Wie op basis van toestemming persoonsgegevens op internet publiceert, 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 verklaring moet in duidelijke en begrijpelijke taal zijn opgesteld, goed vindbaar zijn en bij voorkeur op te roepen vanuit elk onderdeel van de publicatie.

In navolging van de aanbeveling van de Artikel 29-werkgroep over het online verzamelen van gegevens[52)], moet een privacyverklaring bij een publicatie op internet minimaal de volgende elementen bevatten:

1 de identiteit, het fysieke en het elektronische adres van de voor de verwerking verantwoordelijke;
2 het doel (de doeleinden) van de verwerking waarvoor de verantwoordelijke gegevens verwerkt via een publicatie op internet;
3 vermelding of het verstrekken van bepaalde informatie verplicht of facultatief is;
4 de ontvangers of de categorieën ontvangers van de verzamelde informatie;
5 vermelding van het recht dat betrokkenen hebben om, afhankelijk van de situatie, toestemming te geven voor of zich te verzetten tegen de verwerking van persoonsgegevens en van de voorwaarden die daarvoor gelden; vermelding van het recht op toegang tot en rectificatie en verwijdering van gegevens. Daarbij moet duidelijk worden gemaakt tot welke persoon of dienst betrokkenen zich moeten wenden om deze rechten uit te oefenen;
6 de naam en het adres (fysiek en elektronisch) van de dienst of persoon die verantwoordelijk is voor het beantwoorden van vragen betreffende de bescherming van persoonsgegevens;
7 informatie over het gebruik van eventuele automatische procedures voor informatievergaring (bijvoorbeeld ten aanzien van het vastleggen van IP-adressen van bezoekers van een website of de inzet van cookies);
8 informatie over het beveiligingsniveau van een publicatie gedurende alle verwerkingsstadia (belangrijk bij publicaties voor een beperkte doelgroep), inclusief verduidelijking of en zo ja, in welke mate, gegevens indexeerbaar zijn voor zoekmachines;
9 vermelding van de bewaartermijn van persoonsgegevens, inclusief eventuele spelregels ten aanzien van uitsluiting/blacklisting;
10 indien van toepassing: het meldingsnummer waarmee de verwerking is aangemeld bij het CBP.

51) MvT, blz 193: 'Dat betekent dat ook betrokkenen die zich bijvoorbeeld bevinden in de Verenigde Staten, wanneer hun persoonsgegevens worden vergaard, daarover behoren te worden geïnformeerd in de zin van de artikelen 33 en 34 van het wetsvoorstel. Zou zo iemand op enigerlei wijze bemerken dat met overtreding van dit voorschrift persoonsgegevens over hem zijn verwerkt, bijvoorbeeld doordat hij specifiek op hem gerichte reclame ontvangt, dan kan hij in Nederland de rechtsmiddelen aanwenden die deze wet hem toekent.'

52) Artikel 29-werkgroep, WP 43, Aanbeveling inzake bepaalde minimumeisen voor het on line verzamelen van persoonsgegevens in de Europese Unie, goedgekeurd op 17 mei 2001.

In de bijlage bij deze richtsnoeren is een model privacyverklaring opgenomen dat aan deze voorwaarden voldoet. Het gaat daarbij om een model dat gebruikt kan worden voor een discussieforum, waarbij deelnemers hun bijdragen al dan niet onder pseudoniem publiceren en de rechtvaardigingsgrond voor een gerechtvaardigde gegevensverwerking toestemming is.

5.4 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. Ook de e-commerce richtlijn (2000/31/EG) kent een dergelijk absoluut identiteitsvereiste, omgezet in artikel 3:15d van het Burgerlijk Wetboek.[53] Een dergelijk absoluut identiteitsvereiste brengt echter risico's mee voor de privacy van individuele webloggers of critici. Een natuurlijk persoon kan goede redenen hebben om zijn fysieke contactadres niet op internet te willen publiceren, uit angst voor bedreigingen of andersoortige ongevraagde benaderingen.

De aanbeveling van de Artikel 29-werkgroep is vooral gericht op verantwoordelijken die op professionele wijze gegevens verzamelen en verwerken, bijvoorbeeld ten behoeve van direct marketing of andere commerciële dienstverlening. Dat individuen massaal over zouden gaan tot het publiceren van persoonsgegevens op internet, had de werkgroep waarschijnlijk toentertijd niet voorzien. Ook de e-commerce richtlijn is niet gericht op natuurlijke personen, maar op commerciële dienstverleners, die 'gewoonlijk tegen vergoeding' hun diensten verrichten.[54]
In het geval van publicaties door natuurlijke personen is een nadere afweging noodzakelijk om recht te doen aan de goede redenen die een verantwoordelijke kan hebben om zijn fysieke contactadres niet te willen publiceren op internet. Het CBP acht het daarom een redelijke wetstoepassing als een natuurlijke persoon die zonder commercieel oogmerk op internet publiceert, volstaat met het bekendmaken van een elektronisch contactadres. Daarbij gelden twee voorwaarden:

- de verantwoordelijke is goed bereikbaar voor betrokkenen door middel van een elektronisch e-mailadres;
- dit e-mailadres wordt uitgegeven door een in Nederland gevestigde aanbieder.

Een dergelijke verantwoordelijke (die als privépersoon, zonder commercieel oogmerk publiceert) kan niet volstaan met het vermelden van een (veelal gratis) e-mailadres van een internationaal opererende serviceprovider als Microsoft, Google of Yahoo. Een dergelijk adres kan het voor een betrokkene onnodig ingewikkeld maken om zijn recht te halen als een verantwoordelijke niet adequaat reageert.
Het e-mailadres moet uitgegeven zijn door een in Nederland gevestigde aanbieder, binnen het Nederlandse .nl domein. Verantwoordelijken die over een eigen mailserver beschikken kunnen eveneens aan deze verplichting voldoen, mits zij de e-mail verwerken onder een .nl domein.

Het vereiste van een Nederlands elektronisch contactadres maakt het voor betrokkenen mogelijk om nadere stappen te ondernemen om de identiteit te achterhalen van de verantwoordelijke. Het Lycos-arrest van het Hof Amsterdam[55] kan de betrokkene een aanknopingspunt bieden om de provider aan te spreken als de verantwoordelijke voor een publicatie op internet zijn identiteit niet kenbaar maakt

53) 3:15d eerste lid BW: 'Degene die een dienst van de informatiemaatschappij verleent, maakt de volgende gegevens gemakkelijk, rechtstreeks en permanent toegankelijk voor degenen die gebruik maken van deze dienst, in het bijzonder om informatie te verkrijgen of toegankelijk te maken:
a. zijn identiteit en adres van vestiging;
b. gegevens die een snel contact en een rechtstreekse en effectieve communicatie met hem mogelijk maken, met inbegrip van zijn elektronische postadres;' (onderdelen c tot en met f niet geciteerd)

54) 3:15d derde lid BW.

55) Arrest van 24 juni 2004 van het Hof Amsterdam, rolnummer 1689/03 KG. Het Hof oordeelde dat hostingprovider Lycos de persoonsgegevens van een abonnee aan X. moest verstrekken. De abonnee had X. voor oplichter uitgemaakt op zijn website. Het Hof oordeelde dat het voldoende aannemelijk was dat de uiting onrechtmatig zou kunnen zijn en dat Lycos daarom onrechtmatig handelde door de persoonsgegevens van de abonnee niet te verstrekken. Eind 2005 verwierp de Hoge Raad het door Lycos ingestelde cassatieberoep, waardoor het arrest van het Hof definitief werd. De Hoge Raad merkte wel op dat het met die verwerping geen algemene regel wilde formuleren over een verplichting tot het verstrekken van persoonsgegevens aan derden, Hoge Raad der Nederlanden, 25 november 2005, LJN: AU4019, C04/234HR

en daarmee onmiskenbaar in strijd handelt met artikel 33 en 34, tweede lid Wbp.[56)]

Voor privépersonen die geen Nederlands e-mailadres willen gebruiken, geldt de volledige informatieplicht om zowel een fysiek als een elektronisch contactadres bekend te maken.

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.[57)] Echter, de meldingsplicht uit de Wbp (en de onderliggende Europese privacyrichtlijn) dateert van voor de massale opkomst van bijvoorbeeld weblogs en andere populaire internetpublicatievormen, zoals websites van verenigingen en bedrijven. 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, maar deze zijn wel in de maak (zie hieronder paragraaf 6.3). 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.

6.1 Wat betekent een melding?

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 betrekking heeft op het verzamelen, houdt dit in dat de verantwoordelijke de verwerking moet melden voordat hij de beschikking krijgt over persoonsgegevens.[58)]
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.

6.2 Vrijstellingsbesluit

Via het Vrijstellingsbesluit[59)] worden allerlei bekende, veel voorkomende vormen van gegevensverwerking waarvan het bestaan in het algemeen bekend mag worden verondersteld en die geen bijzondere risico's meebrengen, vrijgesteld van de meldingsplicht. De vrijstellingen zijn in het algemeen echter niet relevant voor de publicatie van persoonsgegevens op internet, zodat daarop hier verder niet wordt ingegaan.

6.3 Toekomst: uitbreiding vrijstellingen internetpublicaties

Het ministerie van Justitie heeft in 2007 gewerkt aan een verruiming van het Vrijstellingsbesluit. Naar verwachting hoeven stichtingen en verenigingen die persoonsgegevens publiceren op hun eigen website evenals particulieren die persoonlijke publicaties verzorgen, in de toekomst hun verwerkingen onder bepaalde voorwaarden niet te melden. Onder 'persoonlijke publicaties' worden verstaan: publicaties die persoonlijk van aard zijn, niet-commercieel en voor privédoeleinden opgezet. Als aanvullende voorwaarde voor de nieuwe meldingsvrijstellingen geldt dat persoonsgegevens onmiddellijk verwijderd moeten worden als een betrokkene bezwaar maakt tegen de vermelding van zijn of haar persoonsgegevens. Bovendien is van belang dat de pagina's met persoonsgegevens afgeschermd zijn tegen verwerking door zoekmachines, om onverenigbaar gebruik te voorkomen.

56) Overigens bleek in deze zaak dat de abonnee valse contactgegevens had opgegeven. Het Hof benadrukte dat er geen registratieplicht bestaat voor aanbieders van elektronische communicatiediensten. De verplichting tot het bekendmaken van een .nl adres biedt dan ook geen sluitende methode om de identiteit vast te stellen van een verantwoordelijke, maar maakt het wel makkelijker om -via de provider- de identiteit van een verantwoordelijke te achterhalen.

57) 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'.

58) MvT, blz. 137.

59) Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van melding bedoeld in art. 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp), Staatsblad 2001,250, URL: http://www.cbpweb.nl/indexen/ind_wetten_wbp_vrijstellingsbesluit.stm

Ook onderwijsinstellingen en bedrijven die persoonsgegevens publiceren op een besloten intranet vallen onder de voorgestelde nieuwe vrijstellingen. De vrijstelling omvat eveneens publicatie op een besloten intranet van de zogenaamde 'smoelenboeken', foto's van werknemers of studenten/docenten, mits de plaatsing geschiedt met instemming van de Ondernemingsraad. Het CBP is in juni 2007 geconsulteerd over de aanpassingen van het besluit. De verwachting is dat de wijzigingen nog in 2007 in werking zullen treden.[60)]

De vrijstelling waaraan thans wordt gewerkt, betekent alleen vrijstelling van melding bij het CBP, niet van de verplichting om te voldoen aan de vereisten ten aanzien van een zorgvuldige omgang met persoonsgegevens. De informatieplicht (en daarmee de plicht tot het bekendmaken van de identiteit van de verantwoordelijke en de doelstelling van de verwerking) blijft onverkort van toepassing, evenals de overige bepalingen uit de Wbp .

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.

7.1 Beperkt bewaren

Verantwoordelijken moeten voorafgaand aan de publicatie van persoonsgegevens op internet vaststellen hoe lang zij de gegevens online laten staan of anderszins blijven bewaren. Persoonsgegevens mogen volgens artikel 10 Wbp niet langer bewaard worden in een vorm die het mogelijk maakt betrokkenen te identificeren dan noodzakelijk voor de gestelde (gerechtvaardigde) doeleinden.[61)] Volgens het tweede lid van artikel 11 Wbp moet de verantwoordelijke zich bovendien inspannen om ervoor te zorgen dat persoonsgegevens juist en nauwkeurig zijn. Hoe ouder de gegevens zijn, hoe groter de kans dat ze onjuist zijn en daardoor onnodige schade kunnen berokkenen aan betrokkenen. Verantwoordelijken dienen daarom bij elke publicatie van persoonsgegevens af te wegen welke risico's de gekozen beschikbaarheidstermijn met zich meebrengt. Het verdient aanbeveling, ook volgens de Europese Commissie, om te voorzien in een methode om persoonsgegevens na het verstrijken van de vastgestelde termijn automatisch te anonimiseren.[62)]

7.2 Toereikend, ter zake dienend en niet bovenmatig

De verantwoordelijke mag volgens artikel 11 Wbp alleen gegevens verwerken die toereikend zijn, ter zake dienend zijn en niet bovenmatig aan het gestelde doeleinde. In de memorie van toelichting bij de Wbp wordt het voorbeeld genoemd van een winkelier die een registratie opzet van personen die hij heeft betrapt op winkeldiefstal. De winkelier *zal in de regel niet behoeven te registreren welke goederen door de betrokkene uit zijn winkel zijn ontvreemd, wel bijvoorbeeld de waarde daarvan.* Verder mag hij in die registratie geen gegevens opslaan omtrent het (legale) koopgedrag van de betrokken persoon, omdat dat bovenmatig is aan het gestelde doeleinde.[63)] Het voorbeeld heeft alleen betrekking op de eigen registratie door de winkelier. Voor publicatie op internet van lijsten van (vermeende) winkeldieven zal niet snel een rechtvaardigingsgrond in de Wbp gevonden kunnen worden, vanwege de risico's van verdere verwerking door derden.[64)]

60) Nederland is niet het enige land in Europa dat tot een dergelijke verruiming heeft besloten; Frankrijk heeft in 2005 vergelijkbare vrijstellingen voor internetpublicaties gepubliceerd. Zie: CNIL, Délibération n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (Dispense n°6), laatst gewijzigd op 11 mei 2006, URL: http://www.cnil.fr/index.php?id=1928 en Délibération n°2006-130 du 9 mai 2006 décidant de la dispense de déclaration des traitements relatifs à la gestion des membres et donateurs des associations à but non lucratif régies par la loi du 1.5.r juillet 1901 (dispense n°8), laatst gewijzigd op 18 mei 2006, URL: http://www.cnil.fr/index.php?id=2015

61) Zie voor een algemene toelichting op bewaartermijnen het informatieblad 'Bewaartermijnen van persoonsgegevens in uw bestanden' voor verantwoordelijken, en het informatieblad 'Bewaartermijnen van uw persoonsgegevens' voor betrokkenen, beschikbaar via de website van het CBP, URL: http://www.cbpweb.nl, onder 'nieuws en publicaties', 'publicaties', 'informatiebladen'.

62) Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETs), Brussels, 2 mei 2007, COM(2007) 228. "Automatic anonymisation of data, after a certain lapse of time, supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected."

63) MvT, blz. 96-97.

64) Zie de eerder aangehaalde uitspraken over het ophangen van de foto van een vermeende winkeldief, LJN AQ7877, Rechtbank Amsterdam, KG 04/1566 SR en CBP, 30 mei 2006, z2005-0846.

Het feit dat gegevens 'toereikend' moeten zijn, behelst een zorgplicht voor de verantwoordelijke om een zo correct mogelijk beeld te schetsen van een betrokkene over wie hij persoonsgegevens publiceert. Het weglaten van cruciale informatie kan net zo schadelijk zijn voor de persoonlijke levenssfeer als het vermelden van bovenmatige privé details. Als het bijvoorbeeld gaat om een lijst van vermeende wanbetalers kan het weglaten van de vermelding dat en op welke gronden een betrokkene een vordering betwist, die persoon schade berokkenen.

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.[65] De Raad voor de Rechtspraak paste het beleid daarop aan. De toegang tot www.roljournaal.nl is afgebakend. [66]

7.3 Juist en nauwkeurig

Bij het bewaken van de kwaliteit van persoonsgegevens dienen verantwoordelijken ook maatregelen te treffen om er zeker van te zijn dat de gegevens juist en nauwkeurig zijn, in overeenstemming met de werkelijkheid, zonder dat er iets is verdwenen of (ten onrechte) veranderd.[67] Een verantwoordelijke die persoonsgegevens verzamelt en vervolgens publiceert, moet er zeker van zijn dat de gegevens werkelijk door de betrokkene zelf zijn ingevoerd of gewijzigd en niet door een (kwaadwillende) derde. Betrokkenen mogen niet in een positie worden gebracht dat zij moeten ontkennen een bepaalde actie te hebben verricht. Als de aard van de publicatie en de risico´s die ermee gemoeid zijn daartoe noodzaken, dienen verantwoordelijken daarom de identiteit van een aanvrager of gebruiker vast te stellen. Daar bestaan meerdere middelen voor, zoals biometrische toepassingen, PKI Overheid (de public key infrastructure waarbij de overheid certificaten uitgeeft om de identiteit van een gebruiker te waarborgen), DigiD[68] of Open ID (een initiatief om juist van onderop identiteit te waarborgen, door vertrouwen van gebruikers in elkaar). Een ander systeem, dat bijvoorbeeld in Finland en Estland veel gebruikt wordt, is authenticatie via de infrastructuur van internetbankieren.[69] Welk systeem in Nederland het best ingezet kan worden om te voldoen aan de beveiligingsvereisten van de Wbp, is mede afhankelijk van de betrouwbaarheid, de beschikbaarheid, de kosten voor de verantwoordelijke en de gebruikersacceptatie.

7.4 Identiteitsvaststelling alleen elektronisch?

Als de aard van de dienstverlening en de risico's die ermee gemoeid zijn, noodzaken tot het vaststellen van de identiteit, dient de verantwoordelijke zich als eerste af te vragen of het volstaat om alleen elektronische middelen in te zetten, of dat het noodzakelijk is uit het oogpunt van zorgvuldigheid bevesti-

65) 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.

66) 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.'

67) Artikel 11 tweede lid Wbp: De verantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

68) DigiD is één van de systemen die momenteel ontwikkeld worden om de identiteit van een gebruiker op internet vast te stellen. DigiD kent drie zekerheidsniveau's: laag, midden en hoog. Bij het basisniveau volstaat de combinatie van loginnaam en wachtwoord, zoals gebruikt door de Belastingdienst. Inmiddels is gebleken dat deze combinatie niet voldoende uniek is, en ook door derden kan worden gebruikt (Zie de beantwoording van Kamervragen over het gebruik van andermans DigiD bij het invullen van de belastingaangifte, Kamerstukken II, 2006-2007, DGB 2007-01961). Op het middenniveau is een extra code noodzakelijk, die per sms wordt toegestuurd. Deze procedure is bij het schrijven van deze richtsnoeren nog niet beschikbaar voor bedrijven. Voor het hoogste zekerheidsniveau wordt gewerkt aan een elektronische Nederlandse identiteitskaart (eNIK). Het ministerie van Binnenlandse Zaken wil nog in 2007 een kaart ontwikkelen met een chip die door elke Nederlandse ingezetene aangevraagd kan worden bij gemeenten, net zoals een paspoort. De eNIK maakt het mogelijk voor betrokkenen om hun identiteit digitaal kenbaar te maken en aan te tonen.

69) Sinds 2004 maken grote Finse overheidsinstellingen zoals het ministerie van Sociale Zaken, het instituut voor sociale verzekeringen en de belastingdienst gebruik van het identificatiesysteem van internetbankieren. Zie: http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=23144

ging te vragen via een separaat communicatiekanaal. Dat kan via een bevestiging van een betaling die plaatsvindt op initiatief van de aanvrager, of via het aanbrengen van een offline identificatiestap, zoals per brief of telefoon.

7.5 Gebruik identiteitsbewijs

Voor het vaststellen van de identiteit van een betrokkene mag een verantwoordelijke niet zonder meer om een kopie van een identiteitsbewijs vragen. Op paspoort en identiteitskaart staan twee bijzondere persoonsgegevens, waarvan de verwerking in principe verboden is, tenzij een van de wettelijke uitzonderingen van toepassing is, namelijk de pasfoto en het sofinummer (in de toekomst: burgerservicenummer) .

TEVEEL IDENTIFICERENDE GEGEVENS

Om in aanmerking te komen voor de status van 'Gecontroleerde verkoper' bij een bemiddelingswebsite moest een aanvrager bovenmatig veel documenten overleggen. Volgens het CBP kon de verantwoordelijke volstaan met het opvragen van een kopie van een recent bank- of giroafschrift en een kopie van een identiteitsbewijs. Daarbij moest de website de aspirant-verkopers nadrukkelijk wijzen op de mogelijkheid om op die kopieën alle overbodige gegevens onleesbaar te maken. Na verificatie van de identiteit zouden de kopieën moeten worden vernietigd of aan de potentiële Gecontroleerde verkoper worden teruggegeven [70)]

8 Beveiliging

Verantwoordelijken voor publicaties op internet dienen adequate beveiligingsmaatregelen te treffen, zeker als het de publicatie van bijzondere persoonsgegevens betreft. Bij publicaties op internet moet met name rekening worden gehouden met het risico van verdere verwerking voor een ander doeleinde dan het doeleinde waarvoor de gegevens oorspronkelijk zijn verzameld en gepubliceerd.

8.1 Passende beveiligingsmaatregelen

Artikel 13 Wbp verplicht verantwoordelijken tot het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen dienen er mede op gericht te zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Wat een passend beveiligingsniveau is, is afhankelijk van de stand van de techniek, het soort persoonsgegevens, de soort verwerking, de kosten van de tenuitvoerlegging voor de verantwoordelijke en de te verwachten risico's voor betrokkenen. De wetgever heeft nadrukkelijk een open norm gehanteerd, zonder nadere details over de soorten beveiliging. *Dergelijke details zouden sterk tijdgebonden zijn en daarmee afbreuk doen aan het nagestreefde niveau van beveiliging*.[71)]

Om te voldoen aan de beveiligingsnorm van artikel 13 Wbp dienen verantwoordelijken zich, gegeven de huidige stand van de techniek en de normontwikkeling in eerdere uitspraken van het CBP, bij publicaties op internet te houden aan de volgende vijf verplichtingen:

1 Voorkom de onnodige publicatie van persoonsgegevens.
2 Scherm specifieke pagina's met persoonsgegevens af voor zoekmachines.
3 Gebruik wachtwoorden of een andere passende methode om de doelgroep af te bakenen.
4 Beveilig het gegevenstransport door middel van het SSL-protocol.[72)]
5 Beveilig machine(s) en achterliggende databases tegen onbevoegde toegang door derden.

70) College bescherming persoonsgegevens, Z2006-00957, 2 maart 2007, URL: http://www.cbpweb.nl/documenten/med_20070302_marktplaats.shtml

71) MvT, blz 98-99.

72) Secure Sockets Layer (SSL) is een standaard protocol dat gebruik maakt van 'public key encryption' technologie, om een veilige service te zorgen tussen internet-servers, waarbij zowel de privacy van het bericht, de integriteit van het bericht als de verificatie cq. legitimatie van verzender/ontvanger worden gewaarborgd.

8.2 Tegengaan onnodige publicatie persoonsgegevens

Verantwoordelijken hebben uit beveiligingsoogpunt de plicht om maatregelen te treffen om 'onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen' (Artikel 13 Wbp, derde volzin). Soms heeft een verantwoordelijke wel een goede rechtvaardigingsgrond voor het verzamelen en binnen de organisatie verwerken van bepaalde persoonsgegevens, maar leent dat doeleinde zich niet voor integrale publicatie van de persoonsgegevens op internet. Per persoonsgegeven moet daarom een afweging worden gemaakt van de noodzaak van publicatie op internet, in het licht van de te verwachten risico's voor de betrokkene. De plicht tot dataminimalisatie geldt in het bijzonder voor overheden en verantwoordelijken voor openbare registers, omdat betrokkenen in die gevallen minder mogelijkheden hebben om zich te verzetten tegen een specifieke publicatie.[73)]

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.[74)] In de wet wordt een onderscheid gemaakt tussen de verplichte opname van sommige persoonsgegevens in het register en de publicatie ervan op internet. Het burger service nummer 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 personen niet langer via internet worden getoond. Dat werpt een naar verwachting van de Kamers effectieve drempel op tegen het kopiëren van handtekeningen.*[75)] De staatssecretaris van Economische Zaken nam het amendement meteen over.

8.3 Afscherming persoonsgegevens van 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.[76)]

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 middel van een algemene aanpak, door automatisch een anti-indexeringscode op te nemen in de onderliggende html, of via een individuele oplossing, een constructie waarbij de betrokkene expliciet toestemming geeft voor toegang voor zoekmachines. Die tweede optie is bijvoorbeeld handig voor verantwoordelijken voor profiel-, foto/video- of weblogcommunities, zodat elke betrokkene individueel kan beslissen over de beschikbaarheid van zijn gegevens voor derden.

73) Speciaal voor overheden geldt dat bij de behandeling van de Wbp in de Tweede Kamer kamerbreed de motie Nicolaï is aangenomen waarin de regering nadrukkelijk wordt opgeroepen in haar eigen systemen voor de verwerking van persoonsgegevens privacy enhancing technologies (PET) toe te passen (Kamerstukken II, vergaderjaar 1999-2000, 25 892, nr. 31). In het voorjaar van 2007 heeft de Europese Commissie een een mededeling gepubliceerd waarin zij benadrukt dat het essentieel is dat nationale overheden privacybevorderende technologie inzetten, inclusief dataminimalisatie, ter vergroting van het vertrouwen van burgers, zowel in de opzet van de systemen als in de implementatie (Communication from the Commission to the European Parliament and the Council on promoting data protection by Privacy Enhancing Technologies (PETs), Brussels, 2 mei 2007, COM(2007) 228).

74) Wet van 22 maart 2007, Regels omtrent een basisregister van ondernemingen en rechtspersonen (Handelsregisterwet 2007), Staatsblad 153, 1 mei 2007.

75) Kamerstukken II, 2006–2007, 30656, nr. 20, blz 7, 12 februari 2007.

76) 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">

BESCHULDIGINGEN UIT GOOGLE CACHE VERWIJDEREN

In februari 2007 oordeelde de voorzieningenrechter van de Rechtbank Dordrecht[77] dat een gedaagde zich tot het uiterste moest inspannen om een onterechte beschuldiging verwijderd te krijgen uit de Google cache. De gedaagde meende dat zij was opgelicht en publiceerde dit op haar website. Nadat de betaling was bijgeschreven, verwijderde ze de beschuldigingen, maar via de cache van Google doken de beschuldigingen toch nog op. Hoewel de gedaagde zich had ingespannen om de gegevens te verwijderen, was ten tijde van de zitting nog steeds één kopie vindbaar via de zoekmachine. De rechter beval de gedaagde om binnen twee dagen na betekening van het vonnis de uitlating in de cache van de internetzoekmachine Google te doen verwijderen, op straffe van een dwangsom van 250 euro voor iedere werkdag dat de gedaagde in gebreke zou blijven aan dit vonnis te voldoen.

8.4 Gebruik van wachtwoorden of andere doelgroepafbakening

Verantwoordelijken die persoonsgegevens met een specifiek doel op internet publiceren, moeten zorgen voor een adequate bescherming tegen onrechtmatige kennisneming of verdere verwerkingen ervan door derden. Dat is inherent aan het doelbindingsprincipe. Als het gaat om een publicatie die voor een beperkte doelgroep is bedoeld, zoals leden van een sportvereniging, dient de toegang ook daadwerkelijk tot die doelgroep beperkt te zijn. Naast algemene afscherming van de persoonsgegevens voor zoekmachines dient de verantwoordelijke de specifieke toegang alleen mogelijk te maken voor de doelgroep die in het doeleinde is omschreven. Dat kan in veel gevallen door middel van een wachtwoord, mits het gaat om publicaties zonder bijzondere persoonsgegevens of gegevens die op een andere manier grote risico's meebrengen voor betrokkenen. Verantwoordelijken dienen daarbij te werken met individuele wachtwoorden of toegangscodes, in plaats van met generieke wachtwoorden. Om het risico op onbevoegde toegang verder te verkleinen, moeten de wachtwoorden of toegangscodes een beperkte geldigheidsduur hebben, voldoende 'sterk' zijn en versleuteld worden opgeslagen bij de verantwoordelijke.

Als het echter om publicaties gaat met bijzondere persoonsgegevens, zoals medische dossiers of strafrechtelijke gegevens, is de combinatie loginnaam-wachtwoord te zwak. De verantwoordelijke moet in dat geval zoeken naar andere passende technische mogelijkheden om te waarborgen dat alleen degenen die daartoe gerechtigd zijn, toegang krijgen tot specifieke persoonsgegevens.

WEBSITE MET MEDISCHE DOSSIERS

Eind 2000 onderzocht de Registratiekamer de beveiliging van een bemiddelingswebsite waarop patiënten zelf hun medisch dossier op internet kunnen plaatsen.[78] De website stelt patiënten in staat hun medische gegevens online te controleren en te laten bevestigen door hun arts of apotheker. Artsen, apothekers en andere zorgverleners kunnen zelf ook gegevens aan het dossier toevoegen, met toestemming van de patiënt. Het bedrijf dat verantwoordelijk is voor de gegevensverwerking beheert de wachtwoorden voor de inlogprocedure van de patiënten en zorgverleners.

De Registratiekamer stelde voorop dat verwerking van medische gegevens van patiënten via het internet risico's meebrengt. De combinatie van beveiligingsmaatregelen die het bedrijf had getroffen, was naar het oordeel van de Registratiekamer, gezien de toenmalige stand van de techniek en hetgeen in redelijkheid van het bedrijf kon worden gevergd, vooralsnog voldoende. Het bedrijf had ervoor gekozen om de naam-adres-woonplaatsgegevens van patiënten niet in het digitale dossier op te nemen. Daarnaast waren en zijn zowel de communicatie via internet als de toegang tot de database versleuteld met een 128-bits sleutel en wordt een dossier geblokkeerd na drie foutieve inlogpogingen. Het gebruik van een loginnaam en wachtwoord als toegangsbeveiliging voor het dossier op de site vormde in de ogen van de Registratiekamer echter een zwakke schakel in de beveiliging.

De Registratiekamer schreef: *Toegangsbeveiliging door middel van een loginnaam en wachtwoord wordt in het algemeen als een te laag niveau van beveiliging gezien.*

Voor de toekomst, afhankelijk van de ontwikkeling van de techniek en de acceptatie ervan door burgers, zag de Registratiekamer twee alternatieven: gebruik van biometrische toegangsbeveiliging of gebruik van een zogenaamde challenge-response tokencard, een systematiek zoals die voor thuisbankieren wordt gebruikt. In afwachting van die ontwikkeling, ried de Registratiekamer in ieder geval aan de loginprocedure aan te scherpen. Na toekenning van een nieuw of gewijzigd wachtwoord zou de patiënt bij de eerste inlogpoging verplicht moeten worden zelf een wachtwoord te kiezen.

77) LJN: AZ8818,Voorzieningenrechter Rechtbank Dordrecht , 68382 / KG ZA 07-25

78) Registratiekamer, z2000-00926, 20 juni 2001, http://www.cbpweb.nl/documenten/uit_z2000-0926.stm. De site bestaat nog steeds en maakt nog steeds gebruik van een wachtwoordbeveiliging.

8.4.1 Dictionary attacks

De reden dat de combinatie loginnaam-wachtwoord als zwak wordt gezien, ligt in de mogelijkheid dat geautoriseerde gebruikers de combinatie zelf doorgeven aan derden (soms ook onbewust, via spyware op de computer van de gebruiker), maar ook in zogenaamde *dictionary attacks*. Wachtwoorden zijn over het algemeen versleuteld opgeslagen, maar er bestaat gespecialiseerde software om eindeloos loginpogingen op servers af te vuren. Sommige programma's kunnen tientallen tot honderden miljoenen wachtwoorden per seconde uitproberen. Het werk van de aanvallers wordt vergemakkelijkt omdat het gemiddelde wachtwoord in de praktijk te zwak is. Met slechts 100.000 combinaties (gebaseerd op een basislijst van duizend woorden, met elk honderd veelvoorkomende achtervoegsels) wordt bijna een kwart van alle wachtwoorden al geraden, aldus de gerenommeerde beveiligingsexpert Bruce Schneier.[79)]

8.5 Beveiliging gegevenstransport

Gegevenstransport over internet geschiedt in beginsel via openbare verbindingen. Verantwoordelijken dienen ervoor te zorgen dat het verzamelen van persoonsgegevens via websites beveiligd plaatsvindt, bijvoorbeeld met een https-verbinding. Met het gebruik van een via het SSL-protocol[80)] beveiligde verbinding zijn nauwelijks kosten gemoeid en de inzet ervan beveiligt het verkeer over netwerkknooppunten. Bij een onbeveiligde site bestaat het risico dat derden, voor wie de ingevulde gegevens niet bestemd zijn, de gegevens onderscheppen, bijvoorbeeld via het overnemen van sessies of door datadiefstal op internetknooppunten.

De inzet van een SSL-certificaat is ook van belang voor authenticatie van de website zelf, om het risico op 'phishing' te verkleinen. Sites die onbeveiligd zijn, kunnen makkelijker geïmiteerd worden door sites met vergelijkbare domeinnamen. Daarmee kunnen derden op frauduleuze wijze in bezit komen van persoonsgegevens.

DIGIDOOR

Het CBP deed in 2005 onderzoek naar Digidoor, een initiatief van basisscholen in de gemeente Almere om gegevens over leerlingen op internet te publiceren.[81)] In Digidoor (een afkorting van Digitaal doorstromen) worden gegevens van basisschoolleerlingen verzameld met het doel om de aanmelding bij het vervolgonderwijs makkelijker te maken. De bestanden bevatten veel gevoelige informatie over leerlingen zoals opmerkingen over het niveau van rekenen, taal en lezen, maar ook informatie over faalangst, concentratieproblemen, gezondheidsproblemen en in uitzonderlijke gevallen, problemen met betrekking tot de thuissituatie. De website was zonder nadere versleuteling te benaderen via internet. Over het noodzakelijke beveiligingsniveau was van tevoren niet goed nagedacht. Na negatieve publiciteit troffen de verantwoordelijke scholen snel een aantal concrete maatregelen:

- het installeren van een dedicated server en een versleutelde SSL-verbinding;
- het invullen van de verschillende rollen voor toevoegen en inzien van de informatie en het vaststellen van de bewaartermijn voor (herleidbare) gegevens;
- het opstellen van een brochure met nadere uitleg over de techniek, inhoud en werking van het systeem.

De problemen waren te voorkomen geweest als er van tevoren een goed beveiligingsplan was opgesteld, waarbij ook een dreigingsanalyse was gemaakt.

8.6 Beveiliging machines tegen onbevoegde toegang

Regelmatig komen bekende en onbekende websites negatief in het nieuws omdat de beveiliging onvoldoende is en persoonsgegevens toegankelijk worden die niet voor publicatie zijn bedoeld. Dat kan bijvoorbeeld gebeuren als de URL's die gegenereerd worden na een inlogprocedure een voorspelbaar patroon opleveren. Derden kunnen dan makkelijk andere URL's 'raden' en daarmee toegang verwerven tot persoonlijke informatie van betrokkenen. De beveiliging en inrichting van de server(s) waarop de gegevens staan, vormen daarom een apart punt van zorg. De verantwoordelijke dient ervoor te zorgen dat de machines beveiligd zijn tegen onrechtmatige toegang door derden, door consequent beveiligingsadviezen op te volgen. Dat geldt zowel voor het besturingssysteem als voor de software die op een server draait. Zeker bij de verwerking van bijzondere persoonsgegevens verdient het aanbeveling

79) The Washington Times, 'Chances are your password is at risk', 20 januari 2007.

80) Secure Sockets Layer (SSL) is een standaard protocol dat gebruik maakt van 'public key encryption' technologie, om een veilige service te zorgen tussen internet-servers, waarbij zowel de privacy van het bericht, de integriteit van het bericht als de verificatie cq. legitimatie van verzender/ontvanger worden gewaarborgd.

81) CBP, 27 mei 2005, z2004-1152, URL: http://www.cbpweb.nl/documenten/uit_z2004-1152.shtml

om een strikte scheiding aan te brengen tussen de database waarin de gegevens worden verwerkt en de server waarmee gegevens op internet worden gepubliceerd. De risico's die de publicatie van bijzondere persoonsgegevens meebrengt, rechtvaardigen dat gegevens uit de database alleen versleuteld naar de server mogen worden geleid en pas op cliëntniveau ontsleuteld worden.

TOEGANG TOT DIGITALE JAAROPGAVE

In maart 2007 werd bekend dat de digitale jaaropgaven van het Uitvoeringsinstituut Werknemersverzekeringen (UWV) per ongeluk opvraagbaar bleken door andere klanten, als twee mensen tegelijkertijd inlogden. In de Tweede Kamer werden vragen gesteld over het incident.[82] Het UWV liet de minister van Justitie en het CBP weten dat de digitale beschikbaarstelling werd beëindigd binnen een uur nadat de fout werd ontdekt. Iedereen die per ongeluk andermans jaaropgave had ingezien, werd telefonisch benaderd.

NA PUBLICATIE

9 Verwijderen 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 Hoofdstuk II, par. 4.1.) Persoonsgegevens die bij publicatie juist en nauwkeurig waren, kunnen na verloop van tijd niet meer kloppen en een onvolledig beeld schetsen (zoals: X is woedend op Y, terwijl X het al lang heeft bijgelegd met Y).

Houders van websites of forums zijn onder de Wbp ook verantwoordelijk voor onjuiste of onnodige vermeldingen van persoonsgegevens door de bezoekers van hun publicatie. De verantwoordelijke moet daarom actief modereren om aperte onrechtmatigheden te voorkomen, zeker als het gaat om bijzondere gegevens, zoals strafrechtelijke of gezondheidsgegevens (zie hoofdstuk I paragraaf 8). Om onrechtmatigheid van de publicatie te voorkomen, dienen verantwoordelijken ervoor te zorgen dat bijdragen alleen gepubliceerd kunnen worden op tijdstippen dat er moderatie aanwezig is.

9.1 Plicht tot verwijderen onjuiste gegevens

Op sommige discussieforums worden aparte discussieonderwerpen ('threads' of 'topics') geopend over meldingen die bij nader inzien onjuist zijn gebleken, bijvoorbeeld bij beschuldigingen van spam, oplichterij of andere strafbare feiten. De oorspronkelijke mededelingen met onjuiste persoonsgegevens blijven dan via internet beschikbaar. Het kunnen toevoegen van een andere zienswijze (in plaats van het verwijderen of corrigeren van persoonsgegevens) is een praktijk die in sommige gevallen van toepassing is bij archieven die onder de Archiefwet vallen. Het doeleinde van behoud van (een deel van) het Nederlandse culturele erfgoed maakt het mogelijk om archiefbescheiden met zelfs aantoonbaar onjuiste gegevens voor onbepaalde tijd te bewaren in archiefbewaarplaatsen. Artikel 36 vierde lid Wbp maakt een vergelijkbare werkwijze mogelijk voor gegevensdragers waarin geen wijzigingen kunnen worden aangebracht, zoals CD-roms of microfiches.[83] Voor (niet-journalistieke) publicaties op internet gelden deze uitzonderingen echter niet. De Wbp biedt geen ruimte aan verantwoordelijken voor publicaties op internet om te volstaan met het bijhouden van een apart lijstje van gegevens die kennelijk incorrect zijn. Als de genoemde persoonsgegevens in een bijdrage feitelijk onjuist of bovenmatig zijn aan het gestelde doel, is de publicatie onrechtmatig en moet de bijdrage worden verwijderd.

82) Kamerstukken II, 16 april 2007, UB/S/2007/12116, antwoorden op vragen van de Kamerleden Van Hijum en Omtzigt (CDA).

83) Artikel 36 lid 4 Wbp: 'Indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, dan treft hij de voorzieningen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens op grond van dit artikel.'

BESCHULDIGING VAN OPLICHTERIJ

In een discussieforum over oplichterij wordt mevrouw X beschuldigd door meneer Y van het toesturen van een baksteen in plaats van de beloofde digitale camera. Mevrouw X wordt met naam en toenaam beschreven, inclusief haar vermeende adres, bankrekeningnummer, IP-adres en verwijzingen naar andere beschuldigingen. Mevrouw X blijkt echter verwisseld te zijn met een andere persoon met dezelfde achternaam en voorletter. Ze wil dat alle postings over haar onmiddellijk verwijderd worden van het forum. Is meneer Y dan verantwoordelijk voor die uitlating en moet mevrouw X zich dus tot meneer Y wenden voor correctie of verwijdering? Nee, in termen van de Wbp is de houder van het forum verantwoordelijk voor de persoonsgegevens op het forum. Mevrouw X kan zich in dit geval tot de forumbeheerder wenden om haar persoonsgegevens gecorrigeerd of verwijderd te krijgen. De beheerder van het forum kan een dergelijk verzoek alleen weigeren als hij kan aantonen dat met de publicatie een belang wordt gediend dat groter is dan het recht op bescherming van de persoonlijke levenssfeer van mevrouw X, bijvoorbeeld omdat hij kan aantonen dat er géén sprake is van persoonsverwisseling. De forumbeheerder mag het verzoek niet weigeren met een verwijzing naar een bepaling in de algemene voorwaarden dat bijdragen nooit verwijderd worden. Een dergelijke algemene bepaling is in strijd met de Wbp, omdat er geen individuele belangenafweging aan ten grondslag ligt. De beheerder mag evenmin volstaan met het toevoegen van het weerwoord van mevrouw X aan de lopende discussie.

III

RECHTEN VAN BETROKKENEN

1 **Inleiding** *37*

2 **Inzage** *37*

3 **Correctie en verwijdering** *38*

4 **Recht van verzet** *38*

5 **Uitzondering: openbare registers** *39*

1 Inleiding

Betrokkenen, de natuurlijke personen over wie persoonsgegevens worden gepubliceerd, kunnen ingrijpend benadeeld worden door de onjuiste, onvolledige of onnodige publicatie 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 de publicatie van persoonsgegevens op internet 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.[84)]

2 Inzage

Bij publicaties op internet 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 publicaties waarbij de toegang is afgeschermd. Een betrokkene kan in een dergelijk geval gebruik maken van het inzagerecht om erachter te komen of en zo ja welke gegevens er over hem in een afgeschermde publicatie zijn opgenomen.
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. Het recht op inzage is onder meer van belang voor verantwoordelijken die zwarte lijsten hanteren. Veel populaire publicaties met reactiemogelijkheden of discussiefora bevatten gebruiksregels over toegestaan gedrag. Wie de regels herhaaldelijk of op ernstige wijze overtreedt, kan op een zwarte lijst komen van geblokkeerde IP-adressen en/of gebruikersnamen. De betrokkene heeft dan geen inzicht meer in de gegevens die van of over hem of haar worden gepubliceerd.

De betrokkene heeft het recht zich 'vrijelijk' (dus zonder nadere motivering) en 'met redelijke tussenpozen' tot de verantwoordelijke te wenden met een inzageverzoek.[85)] Het verzoek om kennisneming mag echter niet ongericht zijn.[86)] De verantwoordelijke moet binnen vier weken schriftelijk reageren. Dat mag ook elektronisch.[87)] Het CBP oordeelde in 2003[88)] 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.[89)] De verantwoordelijke mag bij zeer algemene verzoeken om inzage wel om precisering vragen, om een onevenredige 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.[90)] Deze vergoeding moet worden terugbetaald als de verantwoordelijke na de inzage een verbeterings-, vewijderings, aanvullings- of afschermingsverzoek moet honoreren.

84) 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'.

85) Art. 35, eerste lid Wbp

86) MvT, blz. 44

87) Kamerstukken II, nr. 8, blz. 27

88) CBP, z2003-01617. URL: http://www.cbpweb.nl/documenten/med_uit_z2003-1617.shtml

89) Deze interpretatie is medio 2007 bevestigd door de Hoge Raad in de uitspraak over de Dexia-zaak, Hoge Raad, 29 juni 2007, LJN: AZ4663 en Hoge Raad, 29 juni 2007, LJN: AZ4664.

90) Artikel 39 Wbp en het bijbehorende Besluit Kostenvergoeding rechten betrokkene Wbp van 13 juni 2001.

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. Verantwoordelijken moeten een eventuele weigering tot het corrigeren van gegevens met redenen omkleden.

Bij het omgaan met correctieverzoeken maakt het verschil op welke rechtvaardigingsgrond de publicatie is gebaseerd. De betrokkene die toestemming heeft gegeven voor de publicatie (artikel 8 onder a Wbp) kan deze toestemming altijd intrekken (Zie hoofdstuk II, paragraaf 4.1.1). Sites moeten in een dergelijk geval altijd gehoor geven aan een verzoek tot verwijdering en bij de technische inrichting van hun systemen op voorhand rekening houden met deze mogelijkheid. Als de publicatie is gebaseerd op een van de andere rechtvaardigingsgronden uit artikel 8 Wbp, kan een betrokkene om verwijdering of correctie vragen indien de persoonsgegevens feitelijk onjuist zijn, 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.

4 Recht van verzet

Naast het recht op correctie en verwijdering kent de Wbp betrokkenen ook een recht van verzet toe. Dit recht is alleen van toepassing als de publicatie gerechtvaardigd wordt door een rechtvaardigingsgrond onder artikel 8 onder e of f Wbp (de goede vervulling van een publiekrechtelijke taak of de uitkomst van een individuele belangenafweging). Bovenop de bepalingen uit artikel 36 Wbp mag een betrokkene in die gevallen conform artikel 40 Wbp verzet aantekenen tegen de publicatie, met een beroep op bijzondere persoonlijke omstandigheden. Dit 'recht van verzet' heeft betrekking op publicaties die op zich rechtmatig zijn, maar die, door de bijzondere omstandigheden van de betrokkene, onrechtmatig kunnen zijn jegens de betrokkene. Als een betrokkene verzet aantekent, dient de verantwoordelijke een nieuwe, specifieke afweging te maken tussen zijn eigen (gerechtvaardigde) belangen en de belangen van de betrokkene. Indien de betrokkene het niet eens is met het resultaat van die hernieuwde afweging, kan hij de rechter om een beslissing vragen.

Modelverklaring inzage- en correctierecht [91)]
Een verantwoordelijke voor een besloten website met gegevens over wanbetaling in een bepaalde sector brengt betrokkenen via een privacyverklaring op de hoogte van hun rechten op inzage en correctie. Voorop staat dat de betrokkenen moeten zijn geïnformeerd over het doeleinde van de zwarte lijst, de identiteit van de verantwoordelijke en de duur en consequenties van plaatsing vóórdat hun gegevens op de website worden geplaatst, conform de informatieplicht uit artikel 33 en 34 Wbp. De publicatie heeft een rechtvaardigingsgrond in artikel 8 onder f Wbp, om het gerechtvaardigde belang te dienen van een specifieke categorie bedrijven om enige informatie te hebben over het betalingsgedrag van een potentiële klant, alvorens zij overgaan tot het verstrekken van krediet. Betrokkenen kunnen kiezen of zij onjuiste gegevens willen laten verbeteren met een beroep op artikel 36 Wbp, of gebruik willen maken van het recht van verzet van artikel 40 Wbp. Dat laatste kan het geval zijn als de betrokkene bijzondere persoonlijke omstandigheden heeft waardoor hij onevenredig wordt geschaad door opname in de zwarte lijst, ook als de gegevens op zich juist zijn.

Een verklaring over het recht op inzage en correctie kan er als volgt uitzien:

- Inzage in besloten deel website

Indien u uw gegevens wilt inzien in het besloten deel van de website kunt u daartoe een verzoek indienen via privacy@<naamwebsite>.nl. Binnen 7 werkdagen ontvangt u kosteloos bericht of er (nog) gegevens over u verwerkt worden, met welk doeleinde en over welke periode. U kunt ook een gedetailleerde opgave vragen van alle gegevens die op u betrekking hebben. Hieraan wordt binnen vier

91) Deze modelverklaring is geschikt voor particulieren en bedrijven die de publicatie rechtvaardigen met een grondslag onder artikel 8 onder f Wbp, de afweging tussen het gerechtvaardigd belang van de verantwoordelijke versus het recht op bescherming van de persoonlijke levenssfeer van de betrokkene. In dit geval is zowel het recht van verzet van artikel 40 Wbp van toepassing als het recht op correctie of verwijdering uit artikel 36 Wbp.

weken gehoor gegeven. De kosten hiervan bedragen maximaal 4,50 euro, afhankelijk van de hoeveelheid gegevens.

- Recht op verzet

Als u van mening bent dat de verwerking van uw persoonsgegevens in strijd is met de bescherming van uw persoonlijke levenssfeer in verband met uw bijzondere persoonlijke omstandigheden, kunt u dit aangeven via privacy@<naamwebsite>.nl. Als uw verzet gerechtvaardigd is, worden uw gegevens verwijderd. Aan dit verzoek zijn geen kosten verbonden.[92)]

5 Uitzondering: openbare registers

Bij wet ingestelde openbare registers vormen een belangrijke uitzondering op de regel dat betrokkenen zeggenschap hebben over de publicatie van hun persoonsgegevens. 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.[93)] Juist vanwege het ontbreken van een algemene mogelijkheid om bovenmatige 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. In het advies van 15 mei 2007 over de Wet algemene bepalingen omgevingsrecht (Wabo)[94)] 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.*

92) Volgens artikel 40 derde lid Wbp mogen verantwoordelijken voor het in behandeling nemen van een verzet een vergoeding van kosten verlangen, die niet hoger mag zijn dan 4,50 euro, zoals bepaald in het Besluit kostenvergoedingen rechten betrokkenen Wbp (13 juni 2001, Stb. 2001, 305). De vergoeding wordt teruggegeven in geval het verzet gegrond wordt bevonden.

93) 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.

94) CBP, brief aan de leden van de vaste Kamercommissie voor VROM, z2007-00304, 15 mei 2007, http:www.cbpweb.nl/documenten/med_20070515_wabo

IV

TOEPASSELIJKHEID UITZONDERING JOURNALISTIEKE DOELEINDEN

1 **Inleiding** *41*

2 **Afbakening journalistieke exceptie** *41*

3 **Criteria om te beoordelen of de uitzondering van toepassing is** *41*
- 3.1 Objectieve informatieverzameling *42*
- 3.2 Regelmatige bezigheid *42*
- 3.3 Maatschappelijke strekking *42*
- 3.4 Recht van repliek *42*

4 **Archivering van journalistieke publicaties** *43*

5 **Rechter of Raad voor de Journalistiek 43**

1 Inleiding

De Wbp is slechts gedeeltelijk van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden. In deze richtsnoeren wordt alleen de journalistieke exceptie uitgewerkt, aangezien een beroep op artistieke of literaire doeleinden zelden voorkomt.

Niet van toepassing zijn:
- de informatieplicht (artikel 33 en 34 Wbp);
- het verbod op het verwerken van bijzondere persoonsgegevens (artikelen 17 tot en met 23 Wbp);
- de meldingsplicht (artikelen 27 tot en met 30 Wbp);
- de rechten van betrokkenen (artikelen 35 tot en met 42 Wbp);
- het toezicht door het CBP (artikelen 51 tot en met 75 Wbp);
- de beperkingen ten aanzien van doorgifte (artikelen 76 tot en met 78 Wbp).

Wel van toepassing zijn:
- de definities en reikwijdte van de Wbp, inclusief de bepaling over minderjarigheid (artikelen 1 t/m 5 Wbp);
- de plicht om gegevens op behoorlijke en zorgvuldige wijze te verwerken (artikel 6 Wbp);
- de plicht om persoonsgegevens voor welbepaalde en gerechtvaardigde doeleinden te verzamelen (artikel 7 Wbp);
- de plicht tot het hebben van een grond om de gegevensverwerking te rechtvaardigen (artikel 8 Wbp);
- het verbod op onverenigbaar gebruik (artikel 9 Wbp);
- het verbod om gegevens langer te bewaren in een identificeerbare vorm dan noodzakelijk (artikel 10 Wbp);
- het verbod op het verwerken van bovenmatige, niet ter zake dienende persoonsgegevens (artikel 11 Wbp);
- de plicht om passende beveiligingsmaatregelen te treffen (artikel 13 Wbp);
- de bepalingen over de relatie tussen verantwoordelijke en bewerker (artikel 14 Wbp), over toetsing door het CBP van gedragscodes (artikel 25 Wbp) en schadevergoeding (artikel 49 Wbp).

Artikel 3 Wbp is gebaseerd op artikel 9 van de algemene Europese privacyrichtlijn. De Richtlijn stelt uitzonderingen voor de media verplicht, maar 'uitsluitend voor zover deze nodig blijken'. Dat betekent dat lidstaten uitsluitend in uitzonderingen moeten voorzien voor zover ze nodig blijken om een balans te vinden tussen bescherming van de persoonlijke levenssfeer en bescherming van de vrijheid van meningsuiting. Daarom zijn journalistieke publicaties niet vrijgesteld van de algemene zorgvuldigheidsvereisten uit de Wbp, evenals de plicht om maatregelen te treffen om de beveiliging van de verwerking te garanderen.

2 Afbakening journalistieke exceptie

Wanneer valt een publicatie op internet onder de journalistieke exceptie en in welke gevallen is daar geen sprake van? Vaststelling van de grens tussen journalistieke en niet-journalistieke uitingen is van groot belang om te bepalen wanneer het CBP handhavend kan optreden en wanneer andere fora bevoegd zijn, zoals de rechter of de Raad voor de Journalistiek.

3 Criteria om te beoordelen of de uitzondering van toepassing is.

De publicatie van persoonsgegevens op internet valt onder de journalistieke exceptie als zij een uiting is van algemeen maatschappelijk belang die in journalistieke hoedanigheid wordt gedaan (dus niet perse als journalist). Of een uiting met recht en reden een uitsluitend journalistiek doeleinde beweert te dienen, dient te worden beoordeeld door de uiting in zijn context te bekijken en daarna tot een afweging van belangen te komen. Bij die beoordeling hanteert het CBP de volgende criteria:

a is de activiteit gericht op (objectieve) informatieverzameling en verstrekking?
b gaat het om een regelmatige bezigheid?
c gaat het erom iets van maatschappelijke strekking aan de orde te stellen?
d kent de publicatie een recht van repliek of rectificatie achteraf?

Alleen als een publicatie aan alle vier criteria voldoet, is de journalistieke exceptie in ieder geval van toepassing.

3.1 Objectieve informatieverzameling

Is de publicatie gericht op min of meer objectieve informatieverzameling en verstrekking? Bij dit criterium telt niet alleen de publicatie zelf, maar ook de aard van de reacties als het om een interactieve publicatie gaat. Om in aanmerking te komen voor de journalistieke exceptie is van belang of er onderscheid wordt gemaakt tussen feiten, beweringen en meningen, zoals de Raad voor de Journalistiek ook vaststelt in zijn Leidraad.[95] Of een publicatie met reactiemogelijkheid of discussieforum zich kan beroepen op de journalistieke exceptie, hangt mede af van de kwaliteit van de moderatie van reacties van bezoekers. Kan iedere bezoeker van de website vrijuit bijdragen toevoegen die evident schadelijk zijn voor derden, of vindt er controle plaats op de reacties?

3.2 Regelmatige bezigheid

Of een publicist betaald wordt voor zijn publicatie, is niet wezenlijk voor het bepalen van de reikwijdte van de journalistieke exceptie. Het is slechts aan weinigen gegeven om geld te verdienen met een (zelfstandige) publicatie op internet, terwijl met de publicatie wel een groot maatschappelijk belang gediend kan zijn. Beoordeeld wordt of het een regelmatige activiteit betreft. Een weblog met een paar verouderde bijdragen kan zich minder snel beroepen op de journalistieke exceptie dan een publicatie waarop regelmatig nieuwe bijdrages verschijnen.

3.3 Maatschappelijke strekking

Vrij debat over maatschappelijke onderwerpen is van algemeen belang. Uitingen van activisten of belangenorganisaties waarin persoonsgegevens worden verwerkt, kunnen van grote waarde zijn om ernstige misdrijven en misdragingen aan het licht te brengen, om de openbare veiligheid en gezondheid te beschermen en misleiding te voorkomen van het publiek door handelingen en uitspraken van personen of organisaties. Daaruit vloeit evenwel niet voort dat elke dergelijke publicatie van persoonsgegevens op internet een louter journalistiek doeleinde dient.

Of het bij een publicatie van persoonsgegevens gaat om een verwerking voor uitsluitend journalistieke doeleinden, hangt mede af van de overige drie beoordelingscriteria en de hoedanigheid van personen over wie persoonsgegevens worden gepubliceerd. Als een publicatie bijvoorbeeld misdragingen bekendmaakt van een volksvertegenwoordiger of directeur van een bekend of groot bedrijf en de publicatie gebaseerd is op voldoende documentatie om aannemelijk te zijn, dient de publicatie allicht een algemeen maatschappelijk belang. Als een publicatie daarentegen gedetailleerd het privéleven blootlegt van een onbekende persoon, wiens gedragingen niet van invloed zijn op het functioneren van de maatschappij, valt een algemeen belang niet snel te construeren.

3.4 Recht van repliek

Om in aanmerking te komen voor de journalistieke exceptie dient er tenslotte een recht van repliek te zijn.[96] Dat recht houdt in dat betrokkenen een recht van antwoord of rectificatie achteraf hebben van onjuiste informatie, juist omdat de rechten op inzage of correctie niet van toepassing zijn op uitingen met een uitsluitend journalistiek, artistiek of literair doeleinde.

Iedere betrokkene heeft het recht om (kosteloos) te reageren op onjuiste feiten over hem of haar in de media, voor zover die feiten zijn of haar persoonlijke rechten aantasten.[97] De reactie moet een vergelijkbaar prominente plaats krijgen in de publicatie als de oorspronkelijke uiting. De aanbeveling kent een aantal uitzonderingen op de verplichting om de repliek te publiceren; als de repliek veel langer is

95) Leidraad van de Raad voor de Journalistiek, vastgesteld door de leden in april 2007, URL: http://www.rvdj.nl/rvdj-archive/docs/Leidraad_2007.pdf

96) Artikel 29-werkgroep, Aanbeveling 1/97, Wetgeving inzake gegevensbescherming en de media, 25 februari 1997, blz. 8-9: 'De richtlijn vereist een evenwicht tussen twee fundamentele vrijheden.(...) Beperkingen van het recht van toegang en rectificatie voorafgaand aan publicatie kunnen slechts evenredig zijn voor zover de betrokkenen een recht van antwoord of rectificatie van onjuiste informatie hebben na publicatie.'

97) Dit is in lijn met Recommendation Rec(2004)161 of the Committee of Ministers of the Council of Europe to member states on the right of reply in the new media environment, URL: https://wcd.coe.int/ViewDoc.jsp?id=802829. 'Any natural or legal person, irrespective of nationality or residence, should be given a right of reply or an equivalent remedy offering a possibility to react to any information in the media presenting inaccurate facts about him or her and which affect his/her personal rights.'

dan nodig of inhoudelijk niet beperkt tot verbetering van de betwiste feiten. Het recht is ook niet van toepassing als de betrokkene geen geldig belang heeft bij de repliek of als de repliek in een andere taal is gesteld dan de oorspronkelijke publicatie.

Bij de beoordeling of een publicatie onder de journalistieke exceptie valt, dient zwaar mee te wegen of er een recht van repliek is, dan wel anderszins wordt voorzien in een adequaat mechanisme om onjuiste, onvolledige of overbodige persoonsgegevens achteraf te verbeteren of te verwijderen. Het recht van repliek is een laagdrempelige invulling van de journalistieke rectificatienorm[98], die recht doet aan het belang om de journalistieke vrijheid niet op voorhand te beknotten door alle regels uit de Wbp van toepassing te verklaren.

Als betrokkenen echter geen mogelijkheid hebben om achteraf, na publicatie op internet, commentaar te leveren op persoonsgegevens over hen die evident onjuist zijn, kan niet worden aangenomen dat de publicatie een uitsluitend journalistiek doeleinde dient. In dat geval zijn dus alle verplichtingen uit de Wbp van toepassing. De verantwoordelijke voor een niet-journalistieke publicatie kan niet volstaan met het toevoegen van een opmerking van een betrokkene dat gegevens onjuist zijn; hij moet de betreffende persoonsgegevens verwijderen of verbeteren (Zie hoofdstuk II, paragraaf 9.1).

4 Archivering van journalistieke publicaties

Als de publicatie onder de journalistieke exceptie valt, mag de publicatie ook op internet worden gearchiveerd, inclusief bijzondere persoonsgegevens. De journalistieke exceptie werkt 'door' in verdere verwerkingen die plaatsvinden bij bibliotheken en archieven, mits de exploitatie een journalistiek, artistiek of literair doeleinde dient.[99] Als een archief met journalistieke publicaties bijvoorbeeld voor commerciële doeleinden wordt geëxploiteerd, vervalt de exceptie.[100] Bij publicatie op internet van journalistieke archieven met persoonsgegevens is het van belang onderscheid te maken tussen het eerste journalistieke belang van openbaarmaking en het tweede belang van het archiveringsdoeleinde. De verantwoordelijke dient af te wegen voor welke doelgroep hij het archief openstelt en gedurende welke termijn. Ongeacht de toepasselijkheid van de journalistieke exceptie blijven immers de vereisten uit de Wbp van kracht om geen onjuiste of bovenmatige gegevens te publiceren en om behoorlijk en zorgvuldig te werk te gaan.

5 Rechter of Raad voor de Journalistiek

Als een publicatie onder de journalistieke exceptie van de Wbp valt, kan een klacht ofwel door de rechter ofwel door de Raad voor de Journalistiek worden beoordeeld. De rechter toetst of de publicatie voldoet aan de algemene zorgvuldigheidsvereisten uit de Wbp en aan het Burgerlijk Wetboek. De algemene beginselen van zorgvuldigheid van de Wbp hangen nauw samen met de algemene beginselen van maatschappelijke zorgvuldigheid, zoals vastgelegd in het leerstuk van de onrechtmatige daad in het Burgerlijk Wetboek[101] en jurisprudentie.[102]

98) De norm volgens de recente leidraad van de Raad voor de Journalistiek luidt: 'De journalist van wie blijkt dat hij onjuist dan wel op een wezenlijk punt onvolledig heeft bericht, gaat – zo mogelijk op eigen initiatief – op zo kort mogelijke termijn over tot een passende en ruimhartige rechtzetting, die ondubbelzinnig duidelijk maakt dat de berichtgeving in de te rectificeren publicatie of uitzending niet juist was. Indien een betrokkene die zich door de berichtgeving in redelijkheid tekortgedaan voelt, zelf reageert, neemt de redactie de vereiste zorgvuldigheid in acht bij de beslissing of – en zo ja, op welke wijze – de reactie van de betrokkene wordt gepubliceerd.'

99) MvT, blz 73: 'Daarbij valt tevens te denken aan bepaalde gegevensverwerkingen die plaatsvinden bij bibliotheken en musea. Conform de richtlijn worden dergelijke gegevensverwerkingen op één lijn geplaatst met journalistieke gegevensverwerkingen.'

100) MvT, blz 74: 'De exploitatie van op basis daarvan aangelegde gegevensbestanden voor andere dan journalistieke, artistieke of literaire doeleinden valt buiten de reikwijdte van de in artikel 3 geregelde uitzondering.'

101) Artikel 6:162 BW, Lid 1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.
Lid 2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.
Lid 3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

102) Belangrijke jurisprudentie op dit punt is het zogenaamde Gemeenteraadslid-arrest van de Hoge Raad, HR, 24 juni 1983, NJ 1984, 801. Daaruit vloeien zeven, in onderling verband te beschouwen, factoren voort om een afweging te kunnen maken tussen de vrijheid van meningsuiting en het recht op bescherming van de persoonlijke levenssfeer. Zie voor zaken waarin deze criteria zijn toegepast op internetpublicaties ook: LJN: AO2756, Rechtbank Middelburg, 77/2003, 21 januari 2004, LJN: AT4342, Rechtbank Arnhem, 16 maart 2005 en LJN: AY5772, Rechtbank Zwolle, 122465 / KG ZA 06-287, 9 augustus 2006.

De Raad voor de Journalistiek hanteert een eigen maatstaf voor de beoordeling of iets een journalistieke publicatie is. Hij acht zich alleen bevoegd om te oordelen over publicaties van professionele journalisten, dat wil zeggen, mensen die hetzij in dienstverband of als zelfstandige er hun hoofdberoep van maken mede te werken aan de redactionele leiding of redactionele samenstelling van publiciteitsmedia.[103)]

Uit de opsomming van soorten media waarover de Raad voor de Journalistiek kan oordelen, blijkt dat ook internetpublicaties eronder kunnen vallen, *voor zover de inhoud daarvan bestaat uit nieuws, reportages, beschouwing of rubrieken van informatieve aard.*

De Raad voor de Journalistiek neemt alleen klachten in behandeling over uitingen van niet-journalisten als zij voor de publicatie worden betaald en het om regelmatige medewerking gaat, zoals denkbaar bij bijdragen van een medisch specialist aan een vakblad.

103) De RvdJ geeft een definitie van journalistieke gedraging en journalist in artikel 4 van de Statuten van de Stichting Raad voor de Journalistiek. 'Onder journalistieke gedraging [wordt] verstaan een handelen of nalaten van een journalist in de uitoefening van zijn beroep. Voorts wordt onder een journalistieke gedraging verstaan een handelen of nalaten in het kader van journalistieke werkzaamheden van iemand die geen journalist zijnde, regelmatig en tegen betaling meewerkt aan de redactionele inhoud van de in het volgende lid genoemde publiciteitsmedia.'

V

DOORGIFTE BUITEN DE EU

1 **Inleiding** *47*

2 **Passend beschermingsniveau** *47*

3 **Onderscheid toegankelijkheid en doorgifte** *47*

3 **Lindqvist-arrest** *47*

5 **Internationaal intranet** *48*

6 **Behoorlijk en zorgvuldig** *48*

1 Inleiding

Het doorgeven van persoonsgegevens naar landen buiten de EU is verboden, tenzij een van de wettelijke uitzonderingen van toepassing is. Hoewel niet-afgeschermde internetpublicaties in principe 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 publicaties op internet 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.

Alleen verantwoordelijken die expliciet de bedoeling hebben om gegevens door te voeren naar een land buiten de EU, zoals het geval kan zijn bij een intranet met persoonsgegevens van een multinational, dienen zich aan de voorschriften omtrent doorgifte te houden.

2 Passend beschermingsniveau

De norm is dat een verantwoordelijke alleen persoonsgegevens mag doorgeven naar landen buiten de EU als de ontvanger voorschriften naleeft die een passend beschermingsniveau bieden. Of een land aan dat niveau voldoet, wordt bepaald door de Europese Commissie of de Europese Raad. Voorbeelden van landen met een passend beschermingsniveau zijn Argentinië, Canada en Zwitserland. Met de Verenigde Staten zijn specifieke afspraken gemaakt over de doorgifte van informatie van vliegtuigpassagiers en over de doorgifte van persoonsgegevens aan bedrijven die zich hebben verplicht om de Safe Harbour regels toe te passen.[104)]

Er zijn een paar uitzonderingen op de algemene verbodsregel. Doorgifte is bijvoorbeeld toegestaan als de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven of als de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst. De minister van Justitie kan ook - onder bepaling van nadere voorschriften - een specifieke vergunning verlenen voor een doorgifte of categorie doorgiften naar een derde land dat geen passend beschermingsniveau biedt.

3 Onderscheid toegankelijkheid en doorgifte

De Wbp en de Richtlijn kennen geen aparte uitzondering voor de doorgifte van persoonsgegevens via openbaar toegankelijke internetpagina's. Naar de letter van de wet kunnen de meeste verantwoordelijken zich daarom niet op één van de uitzonderingsgronden beroepen en is de doorgifte van persoonsgegevens naar inwoners van de meeste landen buiten de EU onrechtmatig. Dit zou in de praktijk tot onwerkbare situaties leiden.

Het CBP volgt daarom de lijn van het Lindqvist-arrest van het Europese Hof van Justitie[105)] (HvJEG) die ertoe leidt dat de bepalingen over de doorgifte naar landen zonder passend beschermingsniveau niet van toepassing zijn, als het tenminste niet expliciet de bedoeling is van de verantwoordelijke om de gegevens uit te voeren naar dergelijke landen.

4 Lindqvist-arrest

Eind 1998 maakte de Zweedse mevrouw Lindqvist een aantal internetpagina's met informatie over haarzelf en collega's in haar kerkgemeente, waaronder soms hun volledige namen, telefoonnummer, werkzaamheden en liefhebberijen. Verder meldde zij dat een van haar collega's haar voet had bezeerd en met gedeeltelijk ziekteverlof was.

Lindqvist had haar collega's niet van het bestaan van de pagina's op de hoogte gesteld noch hun toestemming gekregen en had de verwerking evenmin gemeld bij de Zweedse toezichthouder. Toen zij vernam dat sommige collega's de bedoelde pagina's niet op prijs stelden, verwijderde zij de gegevens over hen. Toch stelde het openbaar ministerie een strafvervolging in, op grond van het gebruik van

104) De Europese Commissie houdt een actueel overzicht bij van goedgekeurde landen, URL: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (NB! inclusief typefout in URL!)

105) HvJEG, 6 november 2003, zaak C101/01 (Lindqvist)

bijzondere persoonsgegevens zonder rechtvaardigingsgrond, het ontbreken van een melding en de doorgifte naar derde landen.

Op de vraag naar de betekenis van de normen voor doorgifte formuleerde het HvJEG een praktisch antwoord.

Het HvJEG stelde dat de ontwikkeling van internet een nieuwe interpretatie van de normen rechtvaardigt, omdat het niet de bedoeling is van verantwoordelijken van websites om gegevens door te geven naar landen buiten de EU.

'Gezien de ontwikkeling van internet ten tijde van de opstelling van richtlijn 95/46 en het ontbreken van criteria voor het gebruik van internet in hoofdstuk IV, kan niet worden aangenomen dat het de bedoeling was van de gemeenschapswetgever, vooruitlopend op latere ontwikkelingen, het begrip doorgifte van gegevens naar een derde land ook te laten gelden voor de handeling van een persoon in de situatie van Lindqvist die gegevens op een internetpagina plaatst, ook wanneer die gegevens daarmee toegankelijk worden gemaakt voor personen uit derde landen die de technische middelen hebben om zich toegang daartoe te verschaffen.'[106)]

Het Hof overwoog daarbij dat publicatie op internet betekent dat de gegevens beschikbaar zijn in alle derde landen, terwijl de regeling voor doorgifte bedoeld is als een bijzondere regeling voor doorgifte naar een specifiek land. Omdat handelingen 'zoals die van Lindqvist' geen doorgifte vormen, behoeft niet te worden onderzocht of iemand uit een derde land toegang tot de betrokken internetpagina heeft gehad dan wel of de server van die provider zich fysiek in een derde land bevindt.[107)]

5 Internationaal intranet

Het Lindqvist-arrest is nadrukkelijk beperkt tot de voorgelegde zaak, waarbij de specifieke omstandigheden in aanmerking worden genomen. Het EHvJ spreekt van 'handeling van een persoon in de situatie van Lindqvist' en 'handelingen als die van Lindqvist'.

Als het wel de bedoeling is om persoonsgegevens ter beschikking te stellen aan een bepaalde groep personen in een derde land, zijn de normen voor doorgifte wel van toepassing. Dat is bijvoorbeeld het geval bij een werkgever met meerdere vestigingen over de hele wereld, die via een intranet persoonsgegevens ter beschikking stelt aan werknemers in alle vestigingen.

6 Behoorlijk en zorgvuldig

Ook de Franse en de Britse toezichthouder[108)] op de bescherming van de persoonlijke levenssfeer hebben de praktische lijn van het Lindqvist-arrest gevolgd, maar benadrukken dat de extra risico's van brede openbaarmaking op internet het extra belangrijk maken dat verantwoordelijken alle andere waarborgen uit de privacywetgeving respecteren. De Britse information commissioner benadrukt de plicht om behoorlijk en zorgvuldig te werk te gaan. De Franse CNIL benadrukt het belang van de informatieplicht, dat verantwoordelijken voor publicaties waarschuwen dat de kans bestaat dat gegevens opgevraagd kunnen worden in landen buiten de EU zonder passend beschermingsniveau.

In Nederland geldt een vergelijkbare (extra) zorgvuldigheidsverplichting als het gaat om doorgifte naar derde landen. Persoonsgegevens moeten ingevolge artikel 6 Wbp altijd in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.[109)] De formulering sluit aan bij het leerstuk van de onrechtmatige daad in het Burgerlijk Wetboek.[110)] Het gaat om maatschappelijke

106) Idem, Overweging 68.
107) Idem, Overweging 70.
108) Zie voor de Britse uitleg: The Eighth Data Protection Principle and international data transfers
The Information Commissioner's legal analysis and recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor. Version 2.0, 30 juni 2006. Voor de Franse uitleg: Délibération n°2005-276 du 17 Novembre 2005
109) Onder verwerken wordt verstaan elke handeling of geheel van handelingen met betrekking tot persoonsgegevens. Hieronder kan onder meer worden verstaan het verzamelen, vastleggen, ordenen, verstrekken aan derden, kopiëren, bewaren en vernietigen van persoonsgegevens.
110) Artikel 6: 162 BW. Zie noot 101.

zorgvuldigheidseisen om een onrechtmatige daad te voorkomen. Een verantwoordelijke voor een publicatie op internet die behoorlijk en zorgvuldig te werk wil gaan, moet uitdrukkelijk rekening houden met de risico's van verdere verwerking in derde landen en betrokkenen adequaat informeren dat er een kans bestaat dat gegevens opgevraagd kunnen worden in landen buiten de EU zonder passend beschermingsniveau. Dit geldt in het bijzonder als het gaat om risicovolle gegevens over bijvoorbeeld godsdienst of seksuele voorkeur.

VI

HANDHAVING EN DE ROL VAN HET CBP

1 **Inleiding** *51*

2 **Maatregelen door betrokkenen** *51*
- 2.1 Rechtsbescherming onder de Wbp *51*
- 2.2 Andere rechtsmiddelen voor betrokkenen *51*

3 **Handhaving door het CBP** *51*
- 3.1 Bemiddeling, klachtbehandeling en ambtshalve onderzoek *52*
- 3.2 Bestuursdwang en last onder dwangsom *52*
- 3.3 Strafrechtelijke handhaving *52*
- 3.4 Internationaal toezicht *52*

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.

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 hoofdstuk 3 van deze richtsnoeren). Het CBP publiceert gelijktijdig met deze richtsnoeren concrete hulpmiddelen voor betrokkenen, in de vorm van 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, of aangifte doen van bijvoorbeeld smaad.

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. Als de verantwoordelijke echter een bestuursorgaan is, zijn de bezwaar- en beroepsregels uit de Algemene wet bestuursrecht van toepassing.

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.
Ook kan sprake zijn van overtredingen van andere specifieke wetgeving, zoals auteursrecht, portretrecht en databankenrecht. Een ander risico voor een verantwoordelijke die onzorgvuldig omgaat met persoonsgegevens is dat een betrokkene aangifte doet wegens smaad, laster of andere strafbare uitingen zoals racistische uitingen, opruiing en uitingen die in strijd zijn met de openbare orde of de goede zeden.

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.

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[111], 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.[112]

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. Dit gebeurt 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.

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.

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).

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.

111) Voor al zijn toezichthoudende activiteiten, niet alleen bij ambtshalve onderzoeken.
112) Artikel 61 tweede lid Wbp jo. artikel 5:15 Awb

MANAGEMENTSAMENVATTING

Op internet worden op heel veel manieren persoonsgegevens gepubliceerd, door overheidsinstellingen, door bedrijven, door journalisten of door particulieren. 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.

Op internet moeten persoonsgegevens op dezelfde zorgvuldige wijze worden verwerkt als in de offlinewereld. Deze publicatie van het College bescherming persoonsgegevens verschaft duidelijkheid over het toepassen van de Wet bescherming persoonsgegevens (Wbp) in een internetomgeving.

REGELS

In het kort dienen degenen die persoonsgegevens op internet (willen) publiceren, de verantwoordelijken, zich te houden aan de volgende regels.

Voorafgaand aan publicatie:

1 Stel vast of de publicatie 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 publicatie.
De belangrijkste rechtvaardiging voor publicatie is toestemming van de betrokkenen. Als het verkrijgen van die toestemming niet mogelijk is, dienen verantwoordelijken te kunnen onderbouwen dat publicatie is toegestaan op grond van een van de vijf andere rechtvaardigingsgronden. Dit zijn: de uitvoering van een overeenkomst, het nakomen van een wettelijke verplichting, het vrijwaren van een vitaal belang van de betrokkene, het goed kunnen vervullen van een publiekrechtelijke taak, of het behartigen van het gerechtvaardigd belang van de verantwoordelijke. Bij deze vijf rechtvaardigingsgronden 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. 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, het afschermen van persoonsgegevens voor zoekmachines, doelgroepafbakening en het beveiligen van het gegevenstransport.

Volgend op publicatie:

9 Verwijder gegevens als de betrokkene zijn toestemming voor publicatie intrekt. Voldoe tevens 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.
10 Verwijder onrechtmatig gepubliceerde persoonsgegevens. Dit speelt vooral bij publicaties met een reactiemogelijkheid voor bezoekers.

UITZONDERINGEN

Op deze regels voor verantwoordelijken zijn enkele uitzonderingen.

1 De eerste betreft het gebruik van persoonsgegevens voor uitsluitend persoonlijke of huishoudelijke doeleinden. De Wbp is daarop niet van toepassing. Wie van deze uitzondering gebruik wil maken, dient wel zodanige beveiligingsmaatregelen te treffen dat de persoonsgegevens alleen toegankelijk zijn voor een kenbare groep familieleden, huisgenoten of vrienden.
2 De Wbp kent specifieke regels voor publicaties met een historisch, statistisch of wetenschappelijk doeleinde. Wie op deze grond persoonsgegevens op internet wil publiceren, dient de toegang eveneens strikt af te bakenen. Er gelden bovendien nog striktere eisen ten aanzien van *bijzondere* persoonsgegevens.
3 Op de publicatie van persoonsgegevens voor uitsluitend journalistieke doeleinden is de Wbp slechts beperkt van toepassing.
4 De Wbp kent een verbod op doorgifte van persoonsgegevens naar landen buiten de EU waarvoor geen passend beschermingsniveau is vastgesteld. Conform het Lindqvist-arrest van het Europees Hof van Justitie is dit verbod niet van toepassing op publicaties op internet. Het feit dat publicaties op internet toegankelijk zijn in allerlei derde landen, wordt niet als 'doorgifte' beschouwd.
De regels zijn alleen van toepassing op verantwoordelijken die doelbewust persoonsgegevens doorgeven naar een of meerdere derde landen, bijvoorbeeld door middel van een internationaal intranet.

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.

MANAGEMENT SUMMARY

Personal data are published on the Internet by government institutions, companies, journalists or individuals in many different ways. Publications on the Internet are generally accessible worldwide, 24 hours per day, to a potentially extensive and highly varied public. The drawback to the benefit of this general accessibility is that people whose personal data are placed on the Internet, the data subjects, could be at a serious disadvantage due to incorrect, incomplete or unnecessary publication of their personal data.

Personal data must be treated with the same care on the Internet as they are offline. This publication by the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] provides clarity with regard to the application of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] in cases involving the Internet.

REGULATIONS

In brief, those persons who (wish to) publish personal data on the Internet, the controllers, must adhere to the following regulations.

Prior to publication:

1 Determine whether the publication serves a legitimate purpose and whether that purpose is consistent with the purpose for which the data were originally obtained.
2 Ensure that publication of the data is justified.
The most important justification for publishing personal data is the consent of the data subjects. If obtaining consent is not possible, the controllers must be able to substantiate that publication is permitted on the basis of one of the other five grounds to make data processing legitimate. These are: to carry out an agreement, to comply with a statutory obligation, to safeguard a vital interest of the data subject, to be able to correctly perform a task under public law, or to uphold the legitimate interests of the controller. For each of these five justifications, it is necessary to establish the necessity of publishing the selected personal data on the Internet.
3 Do not publish sensitive personal data.
Special categories of personal data (sensitive data) are data relating to a person's religion or life principles, race, political persuasions, health, sexual orientation, membership of a trade union, personal criminal records and data relating to wrongful or objectionable behaviour. The publication of special categories of personal data on the Internet is only permitted in the event that the data subject has given his or her express consent or has consciously publicised the data him or herself.

During publication:

4 Observe the obligation to provide information.
Controllers must actively inform the data subjects of the purpose and intention of the publication.
5 Clearly state your own identity, in a manner accessible to each person to visit the publication.
6 Ensure that you do not retain or make available personal data for any longer than is strictly necessary.
7 Actively guarantee the quality and accuracy of the published personal data.
8 Take security measures against unauthorised use.
These measures include data minimisation, protection of personal data from search engines, target group definition and secure transportation of data.

Following publication:

9 Remove data if the data subject withdraws his or her consent to publication.
Comply with requests made by data subjects in respect of access and requests for the deletion, correction, supplementation or blocking of personal data in the event that the data are factually incorrect, incomplete for their purpose or are irrelevant, or have been processed in some other way that contravenes a statutory regulation.
10 Remove wrongfully published personal data. This may particularly apply to publications in which visitors are given the opportunity to respond.

EXCEPTIONS

There are a few exceptions to these regulations for controllers.

1 The first of these relates to using personal data purely for personal or household purposes. The Wbp does not apply to the use of personal data for this purpose. Those who wish to avail themselves of this exception must take security measures to the effect that the personal data are solely accessible to a predefined group of family members, cohabitants or friends.
2 The Wbp comprises specific regulations for publications with a historic, statistical or scientific purpose. Those who wish to publish personal data on this basis must also strictly delimit access. Moreover, stricter requirements apply in respect of sensitive personal data.
3 The application of the Wbp in respect of publishing personal data exclusively for journalistic purposes is limited.
4 The Wbp includes a prohibition regarding the transfer of personal data to countries outside of the EU, for which a suitable level of protection has not been established. In accordance with the Lindqvist judgment of the European Court of Justice, this prohibition does not apply to publications on the Internet. The fact that publications on the Internet are accessible in various other countries is not regarded as 'transfer'. The regulations apply exclusively to controllers that intentionally transfer personal data to one or more countries outside of the EU, for example by means of an international intranet.

SANCTIONS

Controllers who do not comply with the Wbp can be subject to legal action by data subjects, both on the strength of the Wbp and under administrative law and civil law. In addition, they may be subjected to the supervisory powers of the Dutch DPA, varying from mediation to the institution of an official investigation or the imposition of incremental penalties.

MODEL PRIVACYVERKLARING

Voorbeeld privacyverklaring van een discussieforum

Een goede privacyverklaring van een fictieve website met een openbaar discussieforum over een ziekte kan er als volgt uitzien: [113)]

1 Identiteit

De verantwoordelijke voor deze website is de stichting <naam>, Voorbeeldstraat 1, 1000 AB te Haarlem. De stichting is bereikbaar via info@<naamwebsite>.nl

2 Doeleinde

Via deze website en in het bijzonder het discussieforum wil de stichting kennisuitwisseling in de breedste zin bevorderen over de ziekte X, zowel door experts als door geïnteresseerden.

3 Gevraagde informatie

Voor het leveren van bijdragen aan het discussieforum is registratie verplicht. Deelnemers zijn verplicht om hun voor- en achternaam op te geven, e-mailadres, het gewenste wachtwoord en het gewenste pseudoniem waaronder de bijdragen worden gepubliceerd. Bij de registratie wordt tevens het IP-adres vastgelegd en het tijdstip van registratie. Bij elke afzonderlijke bijdrage wordt eveneens het IP-adres en het tijdstip vastgelegd. De aldus verkregen gegevens worden niet op internet gepubliceerd, met uitzondering van het gekozen pseudoniem en de inhoud van de bijdrage. De stichting gebruikt de niet-openbare gegevens om inzicht te krijgen in de soorten gebruikers van de site; om deelnemers in staat te stellen eventuele bijdragen te corrigeren of te laten verwijderen en om eventueel misbruik zoals spamming te bestrijden of om deelnemers uit te sluiten die de gebruiksregels van het forum hebben overtreden. De gebruiksregels zijn te vinden op http://www.<naamwebsite>.nl/gebruiksregels.

Het e-mailadres wordt verder specifiek gebruikt om het gekozen pseudoniem en wachtwoord te bevestigen en eventueel een nieuw wachtwoord toe te sturen. De stichting kan het e-mailadres ook gebruiken om een bericht door te sturen van een andere deelnemer, mits de deelnemer daar toestemming voor heeft gegeven bij de registratie.

De niet-openbare gegevens worden door de stichting niet aan derden verstrekt of voor enig ander doel gebruikt, met uitzondering van wettelijke verplichtingen om desgevraagd gegevens te verstrekken aan bevoegde instanties.

Bij het pseudoniem kan desgewenst een openbaar profiel worden aangemaakt, met nadere informatie over degene die de bijdrage levert, zoals bijvoorbeeld geslacht en leeftijd. Het aanmaken van een profiel is niet verplicht.

4 Ontvangers

De informatie op de website en in het discussieforum is openbaar en wereldwijd toegankelijk. Wie een bijdrage levert, gaat ermee akkoord dat zijn bijdrage door een onbekende groep lezers op onbekende wijze verder verwerkt kan worden. Om eventuele nadelige gevolgen van publicatie te voorkomen, zeker nu het gaat om bijzondere persoonsgegevens met betrekking tot ziekte, verwijdert de stichting bijdragen waarin identificeerbare informatie wordt gepubliceerd over derden. De stichting ontraadt deelnemers ten zeerste om identificeerbare informatie over zichzelf te publiceren.

5 Rechten deelnemers

Deelnemers aan het forum geven door registratie ondubbelzinnige toestemming voor het registreren van hun persoonsgegevens door de stichting en het publiceren op internet van hun bijdrage, inclusief bijzondere persoonsgegevens. Minderjarigen, dat wil zeggen personen onder de zestien jaar, mogen zich alleen registreren met toestemming van hun ouders of voogd. Iedereen kan zijn toestemming te allen tijde intrekken en verzoeken om verwijdering van zijn gegevens. Desgevraagd verwijdert de stichting de gegevens die benodigd waren voor registratie en anonimiseert de stichting bijdragen aan het forum. Dat wil zeggen dat het gekozen pseudoniem wordt vervangen door de generieke term 'verwijderd' en het eventuele bijbehorende profiel wordt gewist. De bijdragen zelf blijven in het forum staan, om de logica van de discussie niet te verstoren, tenzij een deelnemer een bijzondere omstandigheid aanvoert om een specifieke bijdrage te verwijderen, bijvoorbeeld omdat de bijdrage de deelnemer identificeerbaar maakt.

113) Met dit voorbeeld licht het CBP toe hoe de tien elementen van een privacyverklaring in een concreet geval kunnen worden ingevuld. De privacyverklaring staat los van eventueel benodigde algemene voorwaarden of specifieke gebruiksregels. In het kader van privacy by design verdient het de voorkeur om systemen te ontwerpen waarbij geen of zo min mogelijk persoonsgegevens worden verwerkt, dus ook geen verplichte registratie van forumdeelnemers.

Om een verwijder- of correctieverzoek te kunnen uitoefenen, is het noodzakelijk dat de deelnemer de gegevens meldt waarmee hij zich heeft geregistreerd. De stichting neemt contact op met het e-mailadres dat bij registratie is opgegeven.
Het adres voor verwijder- en correctieverzoeken is: privacy@<naamwebsite>.nl

6 Privacyvragen

Vragen over het privacybeleid van de website en het forum kunnen per post aan de stichting worden gesteld, t.1.v. de voorzitter van het bestuur, of per e-mail via privacy@<naamwebsite>.nl

7 Overige gegevensverwerking

De website legt de IP-adressen vast van bezoekers van de website, door middel van een extern statistiekenprogramma. Dat betekent dat alle bezoekers van de website en het forum eerst langs een externe server worden geleid, voor zij op de website van de stichting terechtkomen. De statistieken worden gebruikt om de vindbaarheid en het gebruik van (onderdelen van) de site te meten door bezoekers en de benodigde servercapaciteit in te kunnen schatten. De website gebruikt geen cookies of andere methodes om op geautomatiseerde wijze gegevens te verzamelen.

8 Beveiliging

Voor de registratie van deelnemers aan het forum gebruikt de stichting een beveiligd protocol, https. De aldus verkregen gegevens worden door de stichting opgeslagen in een adequaat beveiligde database, die niet aan internet is verbonden. De gegevens op de website en het discussieforum zijn opgeslagen in een database die met internet is verbonden en adequaat is beveiligd tegen ongeoorloofd gebruik door derden, zoals wijziging van gegevens. Alle gegevens op de website en in het discussieforum zijn openbaar toegankelijk en kunnen dus door elke derde naar zijn eigen systeem worden gekopieerd. De afzonderlijke pagina's met bijdragen zijn niet indexeerbaar voor zoekmachines.

9 Bewaartermijn

Alle gegevens op de website en in het discussieforum blijven beschikbaar op internet zolang de stichting daartoe de middelen en mogelijkheden heeft. Voor een eventuele uitsluiting van het forum geldt een termijn van 1 jaar, gebaseerd op het IP-adres of de IP-adressen van een deelnemer die de gebruiksregels heeft overtreden. Na het verstrijken van 12 maanden wordt het IP-adres of worden de IP-adressen verwijderd uit de blokkadelijst.

10 Melding bij het CBP

De stichting heeft het discussieforum gemeld bij het CBP als een verwerking van bijzondere persoonsgegevens, onder nummer m0000000.

Het College bescherming persoonsgegevens houdt onder de Wet bescherming persoonsgegevens toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Op internet worden veel persoonsgegevens gepubliceerd. Dit document geeft aan hoe het College publicatie van persoonsgegevens op internet in het algemeen beoordeelt. Daarnaast geven de Richtsnoeren uitleg over de wet, aan de hand van illustraties uit de praktijk.

Voor iedereen die publiceert op internet is van belang dat duidelijk is of, wanneer en in welke vorm publicatie 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.

COLOFON

CBP Richtsnoeren
Publicatie van persoonsgegevens op internet
Consultatiedocument
College bescherming persoonsgegevens,
Den Haag, oktober 2007.

Postbus 93374
2509 AJ Den Haag
E-MAIL info@cbpweb.nl

www.cbpweb.nl