# Leidraad

**afstemmen van wetgeving op de**

# Wet bescherming persoonsgegevens

# Inhoudsopgave

# Voorwoord van de Minister van Justitie

Als gevolg van het voortschrijden van ontwikkelingen in de informatie- en communicatietechnologie is gegevensverwerking door de overheid nu op grote schaal en tegen geringe kosten mogelijk. Dat merken we in de wetgevingspraktijk. De verwerking van persoonsgegevens is inmiddels een regelmatig voorkomend beleidsinstrument geworden.

Hoe normaal het mag lijken, gegevensverwerking heeft een bijzondere kant. Het recht op bescherming van het privé-leven, zoals artikel 8, eerste lid, van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden dat formuleert, maakt dat de verwerking van persoonsgegevens ook de bescherming van diezelfde gegevens moet dienen. Verwerking én bescherming van persoonsgegevens zijn echter niet tegengesteld aan elkaar, en ook geen op zichzelf staande absolute waarden. Vaak vergt het inhoud geven aan andere grondrechten, zoals het recht op leven of het recht op veiligheid, dat de wetgever regelt dat persoonsgegevens buiten toestemming van de betrokkene worden verwerkt. Tegelijk verplicht dat de wetgever tot het vaststellen van waarborgen waaronder die verwerking mag plaatsvinden.

Het recht op bescherming van persoonsgegevens is een recht dat in concrete situaties nader moet worden uitgewerkt. Dat is bij uitstek een taak voor de wetgever. De wetgever moet belangen afwegen en zorgen voor een resultaat dat in overeenstemming is met de internationale, de Europese en onze Nederlandse rechtsorde. In die Nederlandse rechtsorde neemt de Wet bescherming persoonsgegevens een aparte plaats in. In die wet zijn de hoofdlijnen neergelegd van het gegevensbeschermingsrecht. Die hoofdlijnen verwijzen naar de plicht tot belangenafweging. De Wet bescherming persoonsgegevens is daarnaast in verband met het legaliteitsbeginsel van bijzonder belang. Bepaalde belangenafwegingen kunnen alleen bij wet in formele zin worden verricht. Om de wetgevingsjurist behulpzaam te zijn bij het voorbereiden van die belangenafweging, en hem ook de weg te wijzen bij een aantal technische aspecten van dat werk, is op initiatief van het Ministerie van Justitie deze leidraad opgesteld.

Ik vertrouw erop dat deze leidraad een plek in de gereedschapskist van de wetgevingsjurist krijgt.

De Minister van Justitie,

E.M.H. Hirsch Ballin

# Inleiding

## *Waarom deze leidraad ?*

De laatste jaren is sprake van een sterke belangstelling voor gegevensverwerking als instrument van overheidsbeleid. Bestuursorganen, toezichthouders en rechtshandhavers hebben persoonsgegevens nodig om hun taken op een voor de samenleving zo min mogelijk belastende wijze uit te kunnen oefenen. Niet zelden is daarvoor een wetsvoorstel nodig waarin informatieverwerking als beleidsinstrument regeling vindt, en dat moet worden afgestemd op de Wet bescherming persoonsgegevens. Dat vraagt gerichte aandacht van de wetgevingspraktijk, want de consequenties van de toepasselijkheid van de Wet bescherming persoonsgegevens moeten natuurlijk wel voldoende duidelijk in beeld worden gebracht. De Minister van Justitie is eerstverantwoordelijke voor de Wet bescherming persoonsgegevens. Bij het Ministerie van Justitie is de nodige kennis geconcentreerd over de Wet bescherming persoonsgegevens. Gegeven het snel toenemende belang van gegevensverwerking als beleidsinstrument, is het van belang de kennis van de Wbp en van de wijze waarop wetgeving op de Wbp moet worden afgestemd onder de aandacht van de wetgevingspraktijk te brengen. Om de wetgevingspraktijk bij die afstemming zo goed mogelijk te ondersteunen, is deze leidraad opgesteld door een werkgroep bestaande uit wetgevingsjuristen van diverse ministeries en van de Raad van State. Het College bescherming persoonsgegevens heeft over deze leidraad een positief advies uitgebracht.

## *Voor wie is de leidraad bestemd?*

Deze leidraad is in de eerste plaats bestemd voor de wetgevingsjuristen die werkzaam zijn op de wetgevingsafdelingen van de ministeries en de Raad van State. Daarnaast bevat deze leidraad ook raadgevingen die voor beleidsambtenaren nuttig zijn. Verder kan de leidraad van nut zijn voor degenen die werkzaam zijn bij instanties die door middel van een adviserende of toezichthoudende rol invloed uitoefenen op de keuzes die aan nieuwe regelgeving ten grondslag liggen. Te denken valt aan het College bescherming persoonsgegevens, dat een adviserende rol heeft bij voorgenomen wetgeving op het gebied van de bescherming van persoonsgegevens, maar ook aan de OPTA of de AFM.

## *Wat is het karakter van de leidraad?*

Deze leidraad is niet bindend. De vaststelling van wetgeving in Nederland is immers zaak van regering en Staten-Generaal, niet van wetgevingsjuristen. De leidraad is echter ook niet geheel vrijblijvend. De Wet bescherming persoonsgegevens is de uitwerking van internationaal en Europees recht, en van de Grondwet. Alleen al dat gegeven maakt dat aan de vaststelling van regelgeving die op de Wet bescherming persoonsgegevens moet worden afgestemd bijzondere eisen worden gesteld, want uit het internationaal en Europees recht en uit de grondrechten vloeien verplichtingen voort die de niet genegeerd kunnen worden.

## *Wat is de leidraad wel en wat is de leidraad niet?*

Deze leidraad gaat over de Wet bescherming persoonsgegevens. De leidraad poogt twee wetgevingsvragen te beantwoorden: (i) hoe stem ik wetgeving af op de Wet bescherming persoonsgegevens en (ii) welke consequenties zijn er verbonden aan de toepassing van die wet waarmee rekening moet worden gehouden. Hoewel die laatste vraag noodzaakt om in de leidraad ook op de inhoud van de Wet bescherming persoonsgegevens in te gaan, beoogt de leidraad uitdrukkelijk niet om een oplossing te bieden voor de vele praktijkvragen rondom de bescherming van persoonsgegevens in individuele gevallen.

## *Hoe kan de leidraad worden geraadpleegd en hoe wordt de leidraad bijgehouden?*

De leidraad is in elektronische vorm beschikbaar via de website van het Kenniscentrum Wetgeving. Een papieren editie is eveneens beschikbaar. Van tijd tot tijd dient de noodzaak zich aan de leidraad bij te werken. Adviezen uit de wetgevingspraktijk daarvoor zijn daarvoor welkom. Zij kunnen worden gericht tot de directie Wetgeving van het Ministerie van Justitie.

# Adviezen voor de wetgevingsjurist

De adviezen die in deze leidraad zijn opgenomen zijn hieronder gerangschikt in een volgorde die zo goed mogelijk aansluit bij de chronologie van het wetgevingsproces.

*Nagaan of aspect van de bescherming van persoonsgegevens reeds is geregeld*

1. Er is al veel geregeld. Ga daarom eerst zorgvuldig na of een voorgenomen wettelijke regeling die aspecten van bescherming van persoonsgegevens moet bevatten niet reeds in de Wet bescherming persoonsgegevens of in andere regelgeving is geregeld. Neem zonodig contact op met de directie Wetgeving van het Ministerie van Justitie indien dit niet op voorhand duidelijk is.

*Terminologie*

2. Denk aan het juiste gebruik van terminologie. Vermijd het gebruik van de term privacy in wettekst en toelichting. Maak waar nodig een onderscheid tussen eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens.

3. Inventariseer bij het opstellen van een ontwerpregeling welk aspect van de eerbiediging van de persoonlijke levenssfeer aan de orde is. Houd rekening met de wijze waarop een en ander door de wetgever reeds is geregeld, respectievelijk is beperkt. Betreft een wetsvoorstel uitsluitend een regeling die betrekking heeft op *persoonsgegevens* of een nadere invulling of beperking van het *recht op bescherming van persoonsgegevens*, dan verdient het de voorkeur om die terminologie in de memorie van toelichting te gebruiken.

*Belangenafweging*

4. Draag in de toelichting bij een regeling die specifiek betrekking heeft op de bescherming van persoonsgegevens zorg voor een expliciete afweging van de in geding zijnde belangen van verantwoordelijken en betrokkenen in relatie tot de doeleinden van gegevensverwerking.

*Grondrechten*

5. Een wetsvoorstel dat een inmenging in het recht op bescherming van het privé-leven, respectievelijk een beperking van het recht op bescherming van de persoonlijke levenssfeer of het recht op bescherming van persoonsgegevens bevat, wordt getoetst op verenigbaarheid met art. 8, tweede lid, EVRM, het Dataprotectieverdrag en art. 10, eerste lid, van de Grondwet. De memorie van toelichting bevat een uitdrukkelijke gemotiveerde weergave van die toets. De eisen aan de motivering zijn zwaarder

naarmate de inmenging in, respectievelijk de beperking van het grondrecht zwaarder is.

6. Betrek in de toelichting op een regeling die een inmenging in het recht op bescherming van persoonsgegevens regelt alle in de paragrafen 2.8.1 tot en met 2.8.6 genoemde onderwerpen.

*Richtlijn nr. 95/46/EG*

7. Bij een voornemen om wetgeving op te stellen die op onderdelen de Wet bescherming persoonsgegevens aanvult of wetgeving op te stellen die daarvan afwijkt, wordt in de memorie van toelichting altijd een expliciete toets aan richtlijn nr. 95/46/EG verricht. De eisen die worden gesteld aan de motivering zijn zwaarder naarmate de aanvulling of de afwijking van de Wbp betekenisvoller is.

8. Over de noodzaak om in een voorgenomen wettelijke regeling met betrekking tot de bescherming van persoonsgegevens van de Wbp of van richtlijn nr. 95/46/EG *afwijkende begrippen* op te nemen wordt voorafgaand overleg gepleegd met de directie Wetgeving van het Ministerie van Justitie.

*Verhouding Wbp tot Wob en Archiefwet*

9. Bij de voorbereiding van wetgeving met betrekking tot de bescherming van persoonsgegevens moet onder ogen worden gezien dat de Wet openbaarheid van bestuur en de Archiefwet 1995 naast de Wbp blijven gelden.

*Begripsbepalingen Wbp*

10. Wanneer de noodzaak vaststaat om in een voorgenomen wettelijke regeling aspecten van de verwerking van persoonsgegevens of van de bescherming van persoonsgegevens op te nemen, wordt daarbij gebruik gemaakt van de in artikel 1 van de Wbp gedefinieerde begrippen, met gebruikmaking van de modelbepaling.

*Bijzondere persoonsgegevens*

11. De wetgevingspraktijk leert dat op de doorbreking van het wettelijk verbod, bedoeld in art. 23, eerste lid, onder e, Wbp regelmatig een beroep wordt gedaan. Daarom volgen hieronder enige richtlijnen en voorbeelden voor het gebruik van deze uitzondering.

12. Allereerst
- artikel 23, eerste lid, onder e, van de Wbp is een *uitzonderingsregeling*; met de toepassing daarvan wordt grote terughoudendheid betracht
- ga daarom eerst zorgvuldig na of de voorgenomen regeling niet reeds valt onder de reeds in de artikelen 17 tem 22 Wbp geregelde doorbrekingen van het verwerkingsver-

bod; *overleg daarover zonodig met de directie Wetgeving van het Ministerie van Justitie*

13. Vervolgens
- ga zorgvuldig na of de voorgenomen regeling niet reeds valt onder de in artikel 23, eerste lid, onder a tot en met d, Wbp geregelde gevallen
- zie voor de vereisten waaraan *toestemming* in de context van de Wbp (en dus ook in de context van art. 23, eerste lid, onder a, van de Wbp) moet voldoen: art. 1, onder i, Wbp
- een volkenrechtelijke verplichting wordt bij of krachtens verdrag of bindend besluit van een volkenrechtelijke organisatie vastgesteld, *een regel van (intern) buitenlands recht is geen volkenrechtelijke verplichting* in de zin van art. 23, eerste lid, onder d, Wbp
- indien het voorstel van wet houdende *wijziging van de Wet bescherming persoonsgegevens in verband met de uitvoering van de op 26 juli 2007 te Washington tot stand gekomen Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers door luchtvaartmaatschappijen aan het Ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), met briefwisseling en verklaring (Trb. 2007, 129)* (Kamerstukken II 2008/09, 31 734, nr. 2) tot wet wordt verheven zal het nieuwe art. 23a Wbp voorzien in een nieuwe uitzonderingsgrond die de overdracht van bijzondere persoonsgegevens mogelijk maakt indien het recht van een derde land daartoe noodzaakt, ook dat kan alleen wanneer daarvoor een zwaarwegend algemeen belang bestaat en passende waarborgen voor de bescherming van de persoonlijke levenssfeer bestaan, maar bovendien is voorzien in een toereikende grondslag krachtens een *verdrag* of *een bindend EU- of EG-besluit*

14. Tenslotte
- wanneer blijkt dat de gewenste voorziening noodzaakt tot het opstellen van nieuwe wetgeving - al dan niet gecombineerd met de aanvraag van een ontheffing bij het College bescherming persoonsgegevens - voorzie dan eerst in een *grondige motivering* van het zwaarwegend algemeen belang en expliciteer welke passende waarborgen voor de bescherming van de persoonlijke levenssfeer worden geboden
- indien *aanvraag van een ontheffing* bij het College bescherming persoonsgegevens wordt overwogen dient daarbij te worden betrokken dat deze ontheffingen uitsluitend voor een beperkte periode worden verleend en dat ten genoege van het College moet worden aangetoond dat er een concreet voornemen bestaat tot legalisatie; naarmate het wetgevingsproces verder is gevorderd en het voornemen daardoor meer is geconcretiseerd, zal deze bewijslast gemakkelijker kunnen worden gedragen
- in het *wetsvoorstel* dienen tenminste expliciet te zijn geregeld: *doeleinde(n) van de voorgenomen gegevensverwerking, omvang van de gegevensverstrekking - zo veel mogelijk te relateren aan specifieke bijzondere persoonsgegevens -, identiteit van de verantwoordelijke, regeling van de verstrekking van gegevens en van de eventueel beoogde verdere verstrekking, mede in relatie tot bestaande wettelijke geheimhoudingsplichten, waarborgen voor de gegevensverstrekking*, (sub) delegatie is gelet op de tekst van art. 23, eerste lid, onder e, Wbp niet aanvaardbaar
- in de *memorie van toelichting* wordt een expliciete *motivering van het zwaarwegend algemeen belang* gegeven en worden de te treffen waarborgen voor de bescherming van de

persoonlijke levenssfeer expliciet uiteengezet
- na afronding van het wetgevingsproces geldt een *notificatieverplichting* voor de betrokken Minister aan de Europese Commissie (art. 23, derde lid, Wbp)

*Gegevensuitwisseling toezichthouders en bestuursorganen*

15. Indien het noodzakelijk is om op structurele basis over te gaan op onderlinge verstrekking van persoonsgegevens tussen bestuursorganen of toezichthouders onderling of tussen bestuursorganen en toezichthouders, behoort aandacht te worden gegeven aan de vraag of de doeleinden voor die verstrekking voldoende zijn bepaald en of er geheimhoudingsplichten bestaan die hieraan in de weg staan.
Zonodig moet een afzonderlijke regeling op het niveau van de formele wet worden getroffen. Zie daarvoor de bijlage bij de brief van de Minister van Justitie van 29 oktober 2008 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2008/09, 31 700 VI, nr. 70), het rapport van de *Werkgroep herijking toezichtsregelgeving*, Den Haag, augustus 2008.
Gebruik bij het ontwerp van een wettelijke regeling de modelbepalingen.
Geef in de toelichting bij een dergelijke regeling in ieder geval een behoorlijk gemotiveerde rechtvaardiging van de beoogde gegevensverstrekking.

*Effecten gebruik bestuursrechtelijke instrumenten Wbp - administratieve lasten*

16. Besteed bij de voorbereiding van wetgeving met betrekking tot de bescherming van persoonsgegevens aandacht aan het effect dat de toepassing van preventieve instrumenten uit de Wbp als de meldplicht en het voorafgaand onderzoek heeft op administratieve lasten en nalevingskosten. Benut waar mogelijk alternatieve mogelijkheden als vrijstelling van de meldplicht of instelling van intern toezicht in plaats van het aanvragen van een voorafgaand onderzoek.
Voor zover de noodzaak mocht bestaan om bij wet of amvb verwerkingen aan te wijzen die aan een voorafgaand onderzoek moeten worden onderworpen wordt afstemming met het Ministerie van Justitie, Directie Wetgeving, gezocht. Op een voorstel van wet of een ontwerpbesluit moet een advies van het College bescherming persoonsgegevens worden gevraagd.

*Transparantieverplichtingen verantwoordelijke*

17. Besteed in voorkomende gevallen in een memorie van toelichting of nota van toelichting aandacht aan de wijze waarop een bestuursorgaan, dat in de desbetreffende wet of algemene maatregel van bestuur als verantwoordelijke voor de verwerking van persoonsgegevens wordt aangewezen, inhoud geeft aan zijn verplichtingen voortvloeiend uit hoofdstuk 5 Wbp.

*Artikel 43 Wbp*

18. Artikel 43 Wbp wordt niet gebruikt als grondslag voor systematische gegevensverstrekking tussen verantwoordelijken. Voor systematische gegevensverstrekking is veelal een afzonderlijke wettelijke regeling noodzakelijk. Artikel 43 Wbp is daarom geen voldoende duidelijke grondslag voor de vaststelling van beleidsregels.

*Grensoverschrijdend gegevensverkeer*

19. Raadpleeg voor nadere informatie over gegevensverkeer met landen buiten de EU en de EER de brief van de Minister van Justitie van 9 maart 2000 aan de voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 1999/2000, 27 043, nr.1). Op de website van het Cbp is ook de nodige achtergrondinformatie te vinden over dit onderwerp.

*Extern toezicht op de naleving van wettelijke bepalingen met betrekking tot bescherming van persoonsgegevens*

20. Het toekennen van toezicht op de naleving van wettelijke bepalingen met betrekking tot de bescherming van persoonsgegevens en die vallen onder de reikwijdte van richtlijn nr. 95/46/EG, van richtlijn nr. 2002/58/EG of van kaderbesluit nr. 2008/977/JBZ, aan andere organen dan het Cbp is alleen in zeer bijzondere gevallen mogelijk. In alle gevallen waarin dit wordt overwogen vindt voorafgaand overleg met de directie Wetgeving van het Ministerie van Justitie plaats.

*Intern toezicht op de naleving van wettelijke bepalingen met betrekking tot bescherming van persoonsgegevens*

21. Overweeg bij de voorbereiding van wettelijke voorschriften met betrekking tot de bescherming persoonsgegevens of het zinvol is een vorm van intern toezicht te regelen. Dat kan door de benoeming van een functionaris voor de gegevensbescherming of een privacyfunctionaris voor te schrijven. Dat kan aanvullend of alternatief door een privacyaudit of een protocolplicht voor te schrijven.

*Vrijstellingsbesluit Wbp*

22. Voorstellen tot aanpassing van het Vrijstellingsbesluit Wbp kunnen, mits voldoende gemotiveerd tot het Ministerie van Justitie, directie Wetgeving, worden gericht. Het Ministerie van Justitie zal deze voorstellen overigens bespreken met het georganiseerd bedrijfsleven en het College bescherming persoonsgegevens.

*Besluit gebruik sofi-nummer*

23. Indien nieuw gebruik van het sofi-nummer wordt overwogen, vindt in verband met de daarvoor noodzakelijke aanpassing van het Besluit gebruik sofi-nummer Wbp voorafgaand overleg plaats met de directie Wetgeving van het Ministerie van Justitie.

# 1. Privacy, eerbiediging van de persoonlijke levenssfeer, bescherming van persoonsgegevens

## 1.1 *Terminologie*

Bij het voorbereiden van wetgeving die raakvlakken heeft met het recht op bescherming van de persoonlijke levenssfeer is het van belang een correcte terminologie te gebruiken en dat ook consequent te doen. Niet zelden wordt de term *privacy* gebruikt. In het normale spraakgebruik heeft privacy een min of meer omlijnde betekenis. Van Dale geeft als omschrijvingen: *"persoonlijke vrijheid; het ongehinderd alleen, in eigen kring, met een partner ergens te vertoeven, gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan"*. Toch is het niet juist in wetteksten en toelichtingen het woord privacy te gebruiken. Daarvoor zijn twee redenen. De eerste is taalkundig. Het gebruik van anglicismen moet zoveel mogelijk worden vermeden. De tweede is staatsrechtelijk. In de Nederlandse wetgeving wordt dit recht als zodanig niet beschermd.
Wel beschermt artikel 10, eerste lid, van de Grondwet het *recht op eerbiediging van de persoonlijke levenssfeer*. Het verdient dan ook de voorkeur om die term te gebruiken wanneer in een wettekst of toelichting dit recht in zijn meest brede zin wordt behandeld.

Een ander aandachtspunt is dat bij de voorbereiding van wetgeving het *recht op eerbiediging van de persoonlijke levenssfeer* goed moet worden onderscheiden van het *recht op bescherming van persoonsgegevens*. Mogelijk vindt het soms door elkaar gebruiken van die begrippen zijn oorzaak mede in de tekst van artikel 10 van de Grondwet, waar in het tweede en derde lid beide rechten met elkaar in verband worden gebracht. Eerbiediging van de persoonlijke levenssfeer is echter een breder begrip dan bescherming van persoonsgegevens. Omgekeerd geldt dat de bescherming van persoonsgegevens niet louter een deelaspect is van de eerbiediging van de persoonlijke levenssfeer. Zo dient de bescherming van persoonsgegevens ook tot uitwerking van het discriminatieverbod.

Advies

Denk aan het juiste gebruik van terminologie. Vermijd het gebruik van de term privacy in wettekst en toelichting. Maak waar nodig een onderscheid tussen eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens.

## 1.2 Verhouding tussen het recht op bescherming van persoonsgegevens en de andere aspecten van het recht op bescherming van de persoonlijke levenssfeer

Het *recht op eerbiediging van de persoonlijke levenssfeer* in brede zin omvat in de hedendaagse staatsrechtelijke dogmatiek verschillende aspecten: een *informationeel* aspect (bescherming van persoonsgegevens), een *fysiek* aspect (bescherming van de lichamelijke integriteit), een *ruimtelijk* aspect (onschendbaarheid van de woning - het huisrecht) en een *communicatief* aspect (bescherming van het brief-, telefoon- en telegraafgeheim). Het is van belang om bij de voorbereiding van wetgeving na te gaan welk aspect van de eerbiediging van de persoonlijke levenssfeer in geding is. In veel gevallen vergt dit enige studie. Met name moet worden nagegaan of de geldende wetgeving al de nodige regels bevat die het desbetreffende grondrecht nader invullen dan wel beperken, of, in het laatste geval, de omstandigheden en procedures van die beperkingen regelt. Soms regelt de wetgever aspecten van horizontale werking. Zie daarover verder paragraaf 2.7.

Advies

Inventariseer bij het opstellen van een ontwerpregeling welk aspect van de eerbiediging van de persoonlijke levenssfeer aan de orde is. Houd rekening met de wijze waarop een en ander door de wetgever reeds is geregeld, respectievelijk is beperkt.
Betreft een wetsvoorstel uitsluitend een regeling die betrekking heeft op *persoonsgegevens* of een nadere invulling of beperking van het *recht op bescherming van persoonsgegevens*, dan verdient het de voorkeur om die terminologie in de memorie van toelichting te gebruiken.

## 1.3 Inhoud van het recht op bescherming van persoonsgegevens

Over de aard van het recht op bescherming van persoonsgegevens het volgende. Het bestaande (grond)wettelijke kader beoogt natuurlijke personen te beschermen tegen de effecten die voortvloeien uit de door de informatie- en communicatietechnologie mogelijk gemaakte grootschalige verzameling en overdracht van gegevens die op hen betrekking hebben. Het doel van artikel 10 van de Grondwet en de Wet bescherming persoonsgegevens (Wbp) is om door het vaststellen van verplichtingen voor verantwoordelijken betrokkenen zo adequaat mogelijk in staat te stellen een zekere controle over het lot van hun persoonsgegevens te bieden. Door het toekennen van een aantal rechten aan de betrokkene wordt deze in staat gesteld die controle daadwerkelijk uit te oefenen. Die controle is niet absoluut. Bij de uitwerking van artikel 10, tweede en derde lid, van de Grondwet in de Wbp is het recht op informationele zelfbeschikking, zoals dit in de Duitse constitutionele rechtspraak is geformuleerd, niet tot uitgangspunt genomen. (Dat recht houdt in dat in de relatie tussen overheid en burger eenieder zelf mag bepalen in hoeverre

informatie over hem wordt gebruikt en bekendgemaakt, met dien verstande dat de wetgever op dat grondrecht in het algemeen belang bepaalde uitzonderingen kan formuleren.)
In de Wbp is noch de handelingsvrijheid van degene die persoonsgegevens verwerkt, noch het recht op bescherming van de gegevens van de betrokken persoon in *abstracto* zwaarwegender.
*In concreto* zal de afweging tussen die belangen moeten worden verricht. Zie Kamerstukken II 1997/98, 25 892, nr. 3, blz. 9.
Dat is belangrijk voor het opstellen van wetgeving. Immers, niet zelden wordt die afweging verricht door wetgever. Het betreft vooral gevallen waarin gegevens van burgers ten behoeve van doeleinden op het gebied van de overheid worden verwerkt. Denk aan openbare registers of basisregistraties. Denk ook aan verplichtingen tot het leveren van gegevens ten behoeve van de uitvoering van fiscale of sociale wetgeving. Dat betekent dat in de memorie van toelichting bij dergelijke wetsvoorstellen die afweging moet worden geëxpliciteerd.

Advies

Draag in de toelichting bij een regeling die specifiek betrekking heeft op de bescherming van persoonsgegevens zorg voor een expliciete afweging van de in geding zijnde belangen van verantwoordelijken en betrokkenen in relatie tot de doeleinden van gegevensverwerking.

## *1.4 Hoofdlijnen verhouding grondwettelijke en wettelijke bescherming van persoonsgegevens*

Artikel 10, eerste lid, van de Grondwet beschermt het *recht op eerbiediging van de persoonlijke levenssfeer* in algemene zin. Artikel 10, tweede en derde lid, van de Grondwet geeft de wetgever opdracht om ter bescherming van dat recht regels vast te stellen in verband met het *vastleggen en verstrekken van persoonsgegevens*, en het recht op *kennisname van personen van over hen vastgelegde gegevens, en het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van die gegevens*.
De wetgever heeft op diverse wijzen uitvoering gegeven aan die regelingsopdracht.
De *Wet bescherming persoonsgegevens* is de algemene regeling waarin artikel 10, tweede en derde lid, van de Grondwet wordt uitgevoerd. De bescherming van gegevens die worden verwerkt in het kader van de politietaak wordt geregeld in de *Wet politiegegevens*, welke wet eveneens expliciet is vastgesteld ter uitvoering van artikel 10, tweede en de derde lid, van de Grondwet.
De bescherming van gegevens die worden verwerkt ten behoeve van de justitiële documentatie en de strafrechtspleging is geregeld in de *Wet justitiële en strafvorderlijke gegevens*. De *Wet op de inlichtingen- en veiligheidsdiensten 2002* regelt in een apart regime de verwerking en

bescherming van persoonsgegevens ten behoeve van de veiligheid van de staat en verwante doelen. Strafrechtelijke bescherming biedt de wetgever door middel van art. 272 van het *Wetboek van Strafrecht*, schending van een geheimhoudingsplicht is een strafbaar feit.

## 1.5 De bescherming van andere grondrechten dan het recht op bescherming van persoonsgegevens in de gegevensbeschermingswetgeving

In de Wbp wordt niet slechts een nadere invulling gegeven aan het recht op bescherming van persoonsgegevens. Ook het *gelijkheidsbeginsel* en het *non-discriminatiebeginsel* worden nader uitgewerkt. Hoofdstuk 2, paragraaf 2, van de Wbp bevat een uitgebreide regeling van bijzondere persoonsgegevens. Het gaat om gegevens betreffende godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, het seksuele leven en gegevens over het lidmaatschap van een vakvereniging, alsmede strafrechtelijke persoonsgegevens. Een onbeperkte verwerking van deze persoonsgegevens kan een negatieve uitwerking hebben op de positie en ontwikkelingsmogelijkheden van individuen. De wetgever heeft daarom de verwerking van bijzondere persoonsgegevens in beginsel verboden, behoudens een wettelijke regeling. Zie daarvoor in het bijzonder de paragrafen 4.7.2 en 5.4 van deze leidraad.
De Wbp kan in dit opzicht ook worden gezien als een bijzondere wet ten opzichte van de *Algemene wet gelijke behandeling* en de *Wet gelijke behandeling op grond van handicap of chronische ziekte*.
In andere wetgeving, bijvoorbeeld in de *Wet op de jeugdzorg*, zijn ten opzichte van de Wbp aanvullende grondslagen opgenomen voor de verwerking van bijzondere persoonsgegevens.
De Wbp kent een algemene exceptie ten behoeve van de *vrijheid van meningsuiting*. De verwerking van persoonsgegevens ten behoeve van journalistieke, artistieke of literaire doeleinden is toegestaan.

# 2. Grondrechtelijk en internationaalrechtelijk kader

De eerbiediging van de persoonlijke levenssfeer, de bescherming van persoonsgegevens daaronder begrepen, wordt gegarandeerd door verschillende verdragen. Sommige daarvan bevatten regels die als eenieder verbindende bepalingen in de zin van artikel 94 van de Grondwet moeten worden aangemerkt. Wanneer wetgeving wordt voorbereid die als een beperking van de persoonlijke levenssfeer moet worden aangemerkt, is het van belang dat die beperking wordt getoetst op verenigbaarheid met die grondrechten.

## 2.1 *Artikel 8 EVRM*

Artikel 8, eerste lid, van het Europees Verdrag ter bescherming van de Rechten van de Mens en de fundamentele vrijheden (Trb. 1951, 154) (hierna: EVRM) formuleert dat eenieder het *recht* heeft op *respect voor zijn privé-leven*, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
De term "privé-leven" heeft dezelfde betekenis als de term "persoonlijke levenssfeer" in de Grondwet. De overige elementen van artikel 8 (familie- en gezinsleven, woning en correspondentie) blijven hier buiten bespreking.
Het EVRM bevat eenieder verbindende bepalingen in de zin van artikel 94 van de Grondwet. Hoewel laatstgenoemd artikel zich in ieder geval tot de rechter richt, en dat artikel hem ook verplicht tot het buiten toepassing laten van met deze verdragsbepaling strijdig recht, is het de vraag of niet ook de wetgever zich aangesproken zou moeten voelen. Het grote belang van het EVRM brengt met zich dat bij voorbereiding van wetgeving daarom bijzondere aandacht behoort uit te gaan naar de verenigbaarheid van wetgeving met het EVRM wanneer sprake is van een regeling die als een inmenging in het recht op respect voor het privé-leven moet worden aangemerkt.

## 2.2 *Artikel 17 IVBPR*

Het IVBPR is een verdrag dat in VN-verband is gesloten. Artikel 17, eerste lid, van het Internationaal Verdrag inzake burgerrechten en politieke rechten (Trb. 1978, 177) (hierna: IVBPR) formuleert dat niemand mag worden onderworpen aan *willekeurige of onwettige inmenging in zijn privé-leven*, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam. De term "privé-leven" in het IVBPR heeft dezelfde betekenis als de term "persoonlijke levenssfeer" in de Grondwet.
Het tweede lid formuleert dat eenieder recht heeft op bescherming "door de wet" tegen inmenging in het in het eerste lid gegarandeerde recht. Dit betekent in de Nederlandse verhoudingen niet dat steeds een formeelwettelijke grondslag aanwezig moet zijn voor een inmenging. De betekenis van art. 8 EVRM is in de praktijk groter dan die van art. 17

IVBPR, aangezien het EVRM, anders dan het IVBPR, voorziet in een rechterlijke instantie - het Europees Hof voor de bescherming van de Rechten van de Mens - die is belast met de uitleg van het verdrag.
Eigenlijk al hetgeen uit art. 17 IVBPR voortvloeit en dat van belang is voor de voorbereiding van wetgeving komt ook terug bij de toetsing van wetgevingsvoornemens aan art. 8 EVRM. Het IVBPR blijft daarom verder buiten beschouwing.

## 2.3 Artikel 8 Handvest van de grondrechten van de Europese Unie

Artikel 8, eerste lid, van het Handvest van de grondrechten van de Europese Unie (PbEU 2007, C 303) formuleert *dat eenieder recht heeft op bescherming van zijn persoonsgegevens*. Het tweede lid van het artikel geeft enige inhoud aan de kwaliteitseisen die gelden voor de verwerking van gegevens ("eerlijk, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet"). Verder formuleert het tweede lid de rechten op inzage en rectificatie. Het derde lid formuleert dat er een onafhankelijke autoriteit moet zijn die op de naleving van deze regels toeziet.
Hoewel het Handvest primair beoogt rechten van de burger te formuleren die deze tegenover de Europese Unie heeft, en hij die dus primair tegen de instellingen en organen van de Unie kan inroepen, blijven ook de lidstaten van Unie niet buiten schot. Het recht op bescherming van persoonsgegevens kan ook tegen de lidstaten worden ingeroepen wanneer die, met inachtneming van het subsidiariteitsbeginsel, het recht van de EU ten uitvoer brengen (artikel 51 Handvest). Dat betekent voor de wetgever tenminste dat bij de implementatie van bindende EU-besluiten op het gebied van gegevensbescherming deze rechten in acht moeten worden genomen.
Uit artikel 6 van het Verdrag betreffende de Europese Unie (hierna: EU) volgt dat aan het Handvest een gelding toekomt die overeenkomt met de tekst van de verdragen. Verwacht mag worden dat op grond van die bepaling het Hof van Justitie van de Europese Unie jurisprudentie zal vormen die van belang zal zijn. Het is op dit moment nog onzeker of de betekenis van de term "de wet" in artikel 8, tweede lid, van het Handvest afwijkt van de betekenis die daaraan in het EVRM wordt gegeven.

## 2.4 Dataprotectieverdrag

Het op 28 januari 1981 te Straatsburg tot stand gekomen *Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens* (Trb. 1988, 7) (ook wel bekend als verdrag nr. 108, hierna: Dataprotectieverdrag) bevat geen normen met een grondrechtelijk karakter. In het Dataprotectieverdrag zijn normen van inhoudelijke en procedurele aard opgenomen met betrekking tot verwerking van persoonsgegevens. Het betreft een aantal belangrijke begripsbepalingen, beginselen met betrekking tot de kwaliteit van persoonsgegevens, bijzondere persoonsgegevens, informatiebeveiliging en transparantie.

Het Dataprotectieverdrag is aangevuld door middel van het op 8 november 2001 te Straatsburg totstandgekomen *Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens, betreffende toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens* (Trb. 2003, 122 en 165). Het Aanvullend Protocol regelt de verplichting tot instelling van een onafhankelijke toezichthouder en de verplichting om grensoverschrijdend gegevensverkeer naar niet bij het Dataprotectieverdrag aangesloten staten uitsluitend toe te staan wanneer in dat derde land een passend regime van gegevensbescherming bestaat.
Het verdrag (met inbegrip van het Aanvullend Protocol) geldt voor Nederland. Voor de positie van de BES-eilanden, die na de staatkundige hervorming van het Koninkrijk immers ook tot Nederland zullen gaan behoren, wordt verwezen naar paragraaf 4.5.5. Het verdrag behoeft wetgeving om te kunnen worden uitgevoerd en heeft mitsdien geen rechtstreekse werking. Overigens is het bepaald denkbaar dat burgers in rechte een beroep doen op het Dataprotectieverdrag. Dat zou kunnen leiden tot het aanmerken van de normen van het Dataprotectieverdrag als eenieder verbindende bepalingen. Het verdrag is in Nederland volledig geïmplementeerd door middel van de Wet bescherming persoonsgegevens.
Bij de voorbereiding van wetgeving moet in verband met het Dataprotectieverdrag in het oog worden gehouden dat het verdrag *minimumnormen* bevat. De in paragraaf 3 van deze leidraad uitgebreid toegelichte EU-richtlijn kent strengere normen.
Een bijzonderheid is dat toetreding tot het Dataprotectieverdrag ook mogelijk is voor staten die niet tot de Raad van Europa behoren.

## 2.5 *Grondwet*

Artikel 10, eerste lid, van de *Grondwet* garandeert het *recht op eerbiediging van de persoonlijke levenssfeer*. In hoofdstuk 1 van deze leidraad is al besproken dat sommige aspecten van de bescherming van de persoonlijke levenssfeer een eigen grondwettelijke regeling kennen in de artikelen 11, 12 en 13 van de Grondwet.
In artikel 10, tweede en derde lid, van de Grondwet geeft de grondwetgever de gewone wetgever twee *regelingsopdrachten*. Daarbij brengt de grondwetgever de bescherming van de persoonlijke levenssfeer in verband met de *bescherming van persoonsgegevens*: ter bescherming van de persoonlijke levenssfeer moeten regels worden gesteld in verband met het vastleggen en verstrekken van persoonsgegevens. Verder moet de wet regels stellen inzake de aanspraak van personen op kennisneming van over hen vastgelegde gegevens en het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van die gegevens. De Wbp dient uitdrukkelijk tot uitvoering van de regelingsopdrachten van de grondwetgever.
Eerbiediging van de persoonlijke levenssfeer is overigens niet beperkt tot de omgang met persoonsgegevens. Zie in dit verband paragraaf 1 van deze leidraad.
Aparte aandacht verdient het *delegatievraagstuk*. Artikel 10, eerste lid, van de Grondwet opent de mogelijkheid tot delegatie bij de regeling van beperkingen van het grondrecht ("bij of krachtens de wet"). Artikel 10, tweede en derde lid, van de Grondwet laten ook

delegatie toe bij de regelingsopdracht ("De wet stelt regels…"). Zie in dit verband ook paragraaf 2.9.

## *2.6 Inmenging en beperking van het recht op eerbiediging van de persoonlijke levenssfeer*

Regelmatig dient zich de noodzaak aan tot het formuleren van wetsvoorstellen waarin een bepaalde inmenging of beperking op de persoonlijke levenssfeer moet worden geregeld. Waar het betreft de bescherming van persoonsgegevens gaat het daarbij niet zelden om het verwerken van persoonsgegevens voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld. Vaak dient zich daarbij de noodzaak aan van het verstrekken van persoonsgegevens van de ene naar de andere verantwoordelijke, buiten toestemming van de betrokkene. Soms moet een regeling worden getroffen voor de verwerking van bijzondere persoonsgegevens.
Dergelijke wetsvoorstellen moeten in beginsel steeds worden aangemerkt als een inmenging, respectievelijk een inbreuk, op de grondrechten van artikel 8 EVRM, respectievelijk artikel 10 van de Grondwet. Uit de jurisprudentie van het EHRM volgt dat dit bijzondere eisen stelt aan de motivering van een dergelijk voorstel. In paragraaf 2.11 zijn bij wijze van illustratie enige relevante arresten van het EHRM genoemd, waarin specifieke eisen zijn gesteld aan de wetgeving die een inmenging regelt. De memorie van toelichting behoort dan ook een uitdrukkelijke - en dus geen impliciete - motivering te bevatten. Omvang en inhoud van de motivering dienen de ingrijpendheid van de inbreuk - zowel naar zwaarte als naar het aantal personen dat het betreft - te weerspiegelen. Het is niet goed mogelijk om in zijn algemeenheid te omschrijven hoe deze eis in de praktijk moet worden toegepast. Belangrijke aandachtspunten zijn in ieder geval de relatieve zwaarte van de inbreuk, de omvang van de kring van betrokkenen, de te volgen procedures, bewaartermijnen, kwaliteit van de gegevens, de aan de betrokkene toekomende rechten van inzage en correctie en het bieden van rechtsbescherming.

Advies

Een wetsvoorstel dat een inmenging in het recht op bescherming van het privé-leven, respectievelijk een beperking van het recht op bescherming van de persoonlijke levenssfeer of het recht op bescherming van persoonsgegevens bevat, wordt getoetst op verenigbaarheid met art. 8, tweede lid, EVRM, het Dataprotectieverdrag en art. 10, eerste lid, van de Grondwet. De memorie van toelichting bevat een uitdrukkelijke gemotiveerde weergave van die toets. De eisen aan de motivering zijn zwaarder naarmate de inmenging in, respectievelijk de beperking van het grondrecht zwaarder is.

## 2.7 Horizontale werking en positie rechtspersonen

Zowel artikel 8 EVRM als artikel 10 van de Grondwet heeft horizontale werking en normeert daarom niet alleen de verhouding tussen de overheid en de burger, maar werkt ook door in de rechtsbetrekkingen tussen burgers onderling. Zo stelt de wetgever ook regels voor de bescherming van de persoonlijke levenssfeer in de relatie tussen arts en patiënt. Zie bijvoorbeeld de artikelen 7:454 tot en met 459 BW. Artikel 8 EVRM biedt in bepaalde gevallen ook bescherming aan rechtspersonen, hoewel die bescherming in beginsel minder vergaand zal zijn dan die aan natuurlijke personen wordt geboden. Ook de bescherming van artikel 10 Grondwet strekt zich uit over rechtspersonen (Kamerstukken II 1976/77, 13 872, nr. 7, blz. 35). De Wbp en de overige gegevensbeschermingswetgeving beschermt rechtspersonen doorgaans niet.

## 2.8 Toets aan artikel 8, tweede lid, EVRM

Artikel 8, tweede lid, EVRM formuleert de eisen waaraan een inmenging in het privé-leven van overheidswege moet voldoen, wil zij gerechtvaardigd zijn. Aan de navolgende elementen moet aandacht worden geschonken bij het opstellen van een memorie van toelichting.

*2.8.1 Terminologie*
Het is bij het opstellen van een memorie van toelichting allereerst van belang de juiste terminologie toe te passen. Het EVRM spreekt van *inmenging*, en niet van een inbreuk.

*2.8.2 Inmenging*
Vervolgens moet de *inhoud en de aard van de inmenging* in de memorie van toelichting worden omschreven. Bij een inmenging in het recht op bescherming van persoonsgegevens zal het in veel gevallen gaan om het verwerken of verstrekken van persoonsgegevens voor andere doeleinden dan de doeleinden waarvoor deze gegevens zijn verzameld, zonder toestemming van betrokkene.

*2.8.3 Openbaar gezag*

De inmenging moet afkomstig zijn van het *openbaar gezag*. Dat wil zeggen dat er sprake moet zijn van een inmenging van *overheidswege*. Een inmenging van *zuiver particuliere aard*, bijvoorbeeld in arbeidsverhoudingen die volledig worden beheerst door het privaatrecht, valt hieronder in beginsel niet. Openbaar gezag is in verband met artikel 8, tweede lid, EVRM een ruimer begrip dan openbaar gezag in de zin van artikel 1:1, eerste lid, onder b, Awb. Zo kan ook de wetgever openbaar gezag uitoefenen, door middel van het vaststellen van algemeen verbindende voorschriften die als een inmenging kunnen worden aangemerkt. Verbodsbepalingen zijn daarvan een voorbeeld. Bedenk dat de wetgever ook kan ingrijpen in de rechtsbetrekkingen tussen burgers onderling. Bedenk ook dat de wetgever soms positieve verplichtingen moet vaststellen om de inhoud van een grondrecht volledig tot gelding te brengen.

*2.8.4 Bij de wet zijn voorzien - kenbaarheid - voorzienbaarheid*

De inmenging moet *bij de wet zijn voorzien*. Het EHRM stelt bij de invulling van dit element niet de eis dat de inmenging bij of krachtens een formele wet moet plaatsvinden. Aan deze eis kan ook zijn voldaan wanneer er sprake is van gedelegeerde regelgeving, regelgeving van decentrale overheden, bekendgemaakte beleidsregels of vaste jurisprudentie. In de jurisprudentie van het EHRM worden nog een aantal aanvullende eisen gesteld. Allereerst het *kenbaarheidsvereiste*. De inmenging moet voor de burger in elk geval kenbaar zijn. Bij wetgeving, verdragen en besluiten van volkenrechtelijke organisaties wordt daaraan steeds voldaan aangezien wetgeving bekendgemaakt wordt in het Staatsblad, de Staatscourant, het Tractatenblad of het Publicatieblad van de Europese Unie. De kenbaarheid van de motivering van wetsvoorstellen is verzekerd dankzij de bekendmaking daarvan in de Kamerstukken. Daarnaast geldt het *voorzienbaarheidsvereiste*. De inmenging moet met voldoende nauwkeurigheid zijn geformuleerd om de burger zo goed mogelijk in staat te stellen zijn gedrag af te stemmen op het geldende recht. Wat de bescherming van persoonsgegevens betreft, betekent dit dat de betreffende wet duidelijk moet aangeven met betrekking tot welke categorieën van personen gegevens mogen worden opgeslagen, onder welke omstandigheden gegevens mogen worden vergaard, en hoe lang deze mogen worden bewaard. Daarnaast dienen er voorzieningen te zijn voor de transparantie en de controleerbaarheid van de opgeslagen informatie, zoals voorschriften voor verslaglegging. Ruim geformuleerde discretionaire bevoegdheden kunnen in dit opzicht problematisch zijn. Tenslotte moet duidelijk zijn met welke sancties overtreders van deze voorschriften rekening moeten houden.

*2.8.5 Noodzakelijk in een democratische samenleving - doelcriteria - dringende maatschappelijke behoefte - proportionaliteit en subsidiariteit*

De inmenging moet *noodzakelijk zijn in een democratische samenleving* in het belang van één of meer van de in artikel 8, tweede lid, EVRM genoemde *doelcriteria*. Genoemd zijn: het belang van de nationale veiligheid, de openbare veiligheid, het economisch welzijn van het land, het voorkomen van wanordelijkheden of strafbare feiten, de bescherming van de gezondheid of de goede zeden en de bescherming van de rechten en vrijheden van anderen. Deze doelcriteria worden in de jurisprudentie van het EHRM doorgaans nogal ruim uitgelegd. Er is een nauwe samenhang tussen de toetsing aan dit element en de toetsing aan het volgende element.

Er is alleen sprake van noodzaak wanneer de inmenging beantwoordt aan een *dringende maatschappelijke behoefte*. De inmenging moet bovendien evenredig zijn aan het nagestreefde doel (*proportionaliteit*) en de daarvoor aangevoerde gronden moeten relevant en toereikend zijn (*subsidiariteit*). Het EHRM laat de lidstaten hierbij in het algemeen een zekere beoordelingsvrijheid. Onbeperkt is deze vrijheid zeker niet.

Een behoorlijke motivering van noodzaak, proportionaliteit en subsidiariteit vormt de kern van de toets aan artikel 8 EVRM. Het verdient aanbeveling aan deze aspecten bijzondere aandacht te geven. De praktijk leert dat de Tweede en Eerste Kamer daaraan veel belang toekennen. (Zie de uitkomst van een door de Eerste Kamer georganiseerde expertbijeenkomst over gegevensbescherming die op 20 maart 2008 plaatsvond, de inzet van de Eerste Kamer daarbij en de reactie van de Minister-President daarop: Handelingen I 2007/08, 31 200 VI, F en Handelingen I 2008/09, nr. 6, blz. 270-271 en 316.)

*2.8.6 Overige aandachtspunten*

Als algemene achtergrond geldt overigens dat de desbetreffende wetgeving ook altijd moet voldoen aan de eisen voortvloeiend uit het recht op toegang tot een daadwerkelijk rechtsmiddel (uiteindelijk de rechter) van artikel 13 EVRM en het discriminatieverbod van artikel 14 EVRM.

Advies

Betrek in de toelichting op een regeling die een inmenging in het recht op bescherming van persoonsgegevens alle in de paragrafen 2.8.1 tot en met 2.8.6 genoemde onderwerpen.

## 2.9 Toets aan artikel 10, eerste lid, van de Grondwet

Ook bij een toets aan artikel 10, eerste lid, van de Grondwet geldt dat in de memorie van toelichting aandacht moet worden geschonken aan het juiste gebruik van de *terminologie*. De Grondwet spreekt van *beperking*, niet van inbreuk.
Bij een grondwettigheidstoets is het belangrijkste element dat, na vaststelling van de omstandigheid dat er sprake is van een beperking van het recht op eerbiediging van de persoonlijke levenssfeer of het recht op bescherming van persoonsgegevens, die beperking *bij* of *krachtens de wet* moet zijn gesteld. Dat betekent dat er een formeelwettelijke grondslag voor de beperking moet bestaan. In dit opzicht stelt de Grondwet een specifieke eis, die geldt naast de eisen voortvloeiend uit het EVRM. Delegatie is toegestaan.
Raadpleeg in dat verband ook de aanwijzingen 22 en 24 van de *Aanwijzingen voor de regelgeving*.

## 2.10 Voorbeelden

Het is in zijn algemeenheid moeilijk aan te geven wanneer aan alle motiveringseisen is voldaan, zodanig dat een voorstel van wet helemaal "Straatsburg-proof" en in overeenstemming met de Grondwet is. Een paar voorbeelden van uitgebreide toetsen zijn opgenomen in de memorie van toelichting bij de volgende wetsvoorstellen.

Voorbeelden

Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens) (Kamerstukken II 2006/07, 31 145, nr. 3, blz. 24 - 27).

Goedkeuring van de op 26 juli 2007 te Washington tot stand gekomen Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het Ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), met briefwisseling en verklaring (Trb. 2007, 129) (Kamerstukken II 2008/09, 31 735, nr. 3, blz. 21 - 23).

Wijziging van de Wet op de jeugdzorg in verband met de introductie van een verwijsindex om vroegtijdige en onderling afgestemde verlening van hulp, zorg of bijsturing ten behoeve van jeugdigen die bepaalde risico's lopen te bevorderen (verwijsindex risico's jeugdigen) (Kamerstukken II 2008/09, 31 855, nr. 3, blz. 8 - 15).

## 2.11 *Een paar belangrijke uitspraken van het EHRM*

De jurisprudentie van het EHRM over artikel 8 EVRM is overvloedig. Aangezien deze leidraad zich richt op de wetgevingspraktijk worden in het onderstaande slechts enkele arresten van het EHRM genoemd die specifieke eisen stellen aan de wetgeving die een inmenging in het recht op bescherming van persoonsgegevens betreft, of dit juist nalaat.

*EHRM 25 februari 1997, Z. tegen Finland, application number 22009/93*

Ten aanzien van het gebruik van opgeslagen medische gegevens ten behoeve van het strafproces heeft het EHRM in deze zaak bepaald dat het belang dat de samenleving heeft bij de opsporing en vervolging van misdrijven kan prevaleren boven het belang van de persoon in kwestie bij geheimhouding van diens gegevens. De reden om over te gaan tot het verstrekken van gegevens moet relevant en toereikend zijn, en evenredig ten opzichte van het te bereiken doel. Ook hier geldt onverminderd dat de betreffende wettelijke regeling waarborgen dient te bevatten ter bescherming van het vertrouwelijke karakter van deze gegevens.

*EHRM 16 februari 2000, Amann tegen Zwitserland, application number 27798/95*

De Zwitserse praktijk van voor 1990 om telefoongesprekken met bepaalde ambassades systematisch af te luisteren en ten aanzien van in Zwitserland verblijvende deelnemers aan die gesprekken een systematische (destijds nog papieren) registratie aan te leggen en deze langdurig te bewaren voor doeleinden verband houdend met de staatsveiligheid, vond onvoldoende basis in de wet. De desbetreffende wetgeving voldeed niet aan de eisen die het EHRM daaraan stelt. De wet behoort regels te bevatten met betrekking tot de afbakening van de kring van personen ten aanzien van wie maatregelen kunnen worden getroffen, de daarbij te hanteren middelen en de daarbij te volgen procedures. Ten aanzien van het aanleggen van de registratie voegde het EHRM daar nog aan toe dat de Zwitserse federale wetgeving voor de bescherming van persoonsgegevens te onbepaald was om de getroffen individuen adequaat te beschermen tegen deze inmenging. Het EHRM oordeelde dat artikel 8 EVRM was geschonden.

*EHRM 4 mei 2000, Rotaru tegen Roemenië, application number 28341/95*

De Roemeense wetgeving die de inlichtingendienst van dat land bevoegdheden toekende tot het verwerken van persoonsgegevens moet als een inmenging in het recht op privéleven worden aangemerkt. Er was sprake van een wettelijke basis voor die inmenging. De wetgeving schoot echter tekort, aangezien deze geen bepalingen bevat die regelen welke soorten van gegevens mogen worden verwerkt, de categorieën van personen van wie persoonsgegevens mogen worden verzameld en bewaard, de omstandigheden waaronder dat mag plaatsvinden en de procedures die daarbij moeten worden gevolgd. Evenmin bevatte de wetgeving een regeling met betrekking tot de actualiteit van de gegevens en

bewaartermijnen. Bovendien ontbrak in de wetgeving een regeling met betrekking tot de beperking van de toegang tot de bewaarde gegevens. Het EHRM kwam tot het oordeel dat sprake was van schending van artikel 8 EVRM.

*EHRM, 3 april 2007, Copland tegen het Verenigd Koninkrijk, application number 62617/00*

In deze uitspraak ging het EHRM verder in op het opslaan van data in een zakelijke context. De klacht in deze zaak was ingediend door een vrouw die werkzaam was aan de open universiteit waar haar telefoon- en internetgebruik werd bijgehouden en nagegaan door haar werkgever, met het doel vast te stellen of dat gebruik bestemd was voor privé-doeleinden. Het EHRM oordeelde dat het feit dat het ging om de registratie van internetgebruik en e-mail gepleegd op de werkvloer, niet afdeed aan het feit dat hier sprake was van een inmenging in de persoonlijke levenssfeer, als bedoeld in artikel 8 EVRM. Voorts was het EHRM van oordeel dat betrokkene een "reasonable expectation of privacy" mocht hebben, nu aan haar geen waarschuwing was gegeven dat het internet- en e-mailgebruik zou worden geregistreerd. Nu in casu een wettelijke grondslag voor die inmenging ontbrak, kwam het EHRM tot het oordeel dat sprake was van een schending van artikel 8 EVRM.

# 3. Europeesrechtelijk kader

## *3.1 Richtlijn nr. 95/46/EG*

Het belangrijkste Europeesrechtelijke kader wordt gevormd door *richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281)*. Een geconsolideerde tekst, waarin een wijziging is verwerkt van de comitologiebepaling, is te vinden in EurLEX, onder nummer 1995L0046 - NL - 20.11.2003 - 001.001 - 1.
Bij de voorbereiding van wetgeving die betrekking heeft op de bescherming van persoonsgegevens moet er nadrukkelijk op worden gelet dat de voorgestelde regeling volledig in overeenstemming is met deze richtlijn. Aangezien de richtlijn in de Wet bescherming persoonsgegevens is geïmplementeerd, dient een toets aan de richtlijn altijd te worden uitgevoerd wanneer een voorstel van wet voorziet in de vaststelling van normen die van de Wet bescherming persoonsgegevens *afwijken* of die de Wet bescherming persoonsgegevens *aanvullen*.
Richtlijn nr. 95/46/EG is een omvangrijke en betrekkelijk moeilijk toegankelijke regeling. Aangezien deze leidraad is geschreven ten behoeve van de Nederlandse wetgevingspraktijk is hier geen inhoudelijke beschrijving van de richtlijn opgenomen. Inhoudelijke behandeling van enkele voor de wetgevingspraktijk belangrijke hoofdzaken van het gegevensbeschermingsrecht volgt hieronder bij de inhoudelijke bespreking van de Wet bescherming persoonsgegevens. In het onderstaande wordt kort ingegaan op de grondslag en de reikwijdte van richtlijn, en enige aan de richtlijn ten grondslag liggen rechtsbeginselen.

Advies

Bij een voornemen om wetgeving op te stellen die op onderdelen de Wet bescherming persoonsgegevens aanvult of wetgeving op te stellen die daarvan afwijkt, wordt in de memorie van toelichting altijd een expliciete toets aan richtlijn nr. 95/46/EG verricht. De eisen die worden gesteld aan de motivering zijn zwaarder naarmate de aanvulling of de afwijking betekenisvoller is.

*3.1.1 Grondslag*
De richtlijn is vastgesteld op grond van artikel 100 A EG-Verdrag (oud), thans artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU).
Op grond van artikel 114 VWEU kunnen door het Europees Parlement en de Raad, volgens de gewone wetgevingsprocedure (“codecisie”), besluiten worden genomen ten behoeve van de onderlinge aanpassing van de wetgeving van de lidstaten die de instelling en de werking van de *interne markt* betreffen.
De richtlijn heeft twee samenhangende hoofddoelstellingen. In de eerste plaats beoogt de

richtlijn de eerbiediging van de *fundamentele rechten en vrijheden* - waaronder de persoonlijke levenssfeer - van natuurlijke personen te bevorderen, ongeacht nationaliteit en verblijfplaats. In de tweede plaats beoogt de richtlijn ten behoeve van het *vrije verkeer* van goederen, personen, diensten en kapitaal het verkeer van persoonsgegevens van de ene lidstaat naar de andere zoveel mogelijk te vergemakkelijken, onder bescherming van de fundamentele rechten van personen.
Het gaat dus om *harmonisatie van wetgeving*. Bij de totstandkoming van de richtlijn bestond er in een groot aantal lidstaten al een wettelijke regeling met betrekking tot persoonsgegevens, veelal ter uitvoering van het Dataprotectieverdrag. In Nederland gold destijds de Wet persoonsregistraties. De richtlijn heeft kenmerken van zowel *minimumharmonisatie* als *partiële harmonisatie*. Zo verwijzen de artikelen 5, 8, vierde en vijfde lid, en 13 van de richtlijn naar de bevoegdheid van de lidstaten tot het stellen van aanvullende of afwijkende regels. Artikel 27 bevordert het gebruik van gedragscodes: private normen op sector- of brancheniveau. De reikwijdte van de richtlijn is niet onbeperkt, zodat er van totale harmonisatie geen sprake is.
Artikel 114, vierde en vijfde lid, VWEU biedt enige, overigens zeer streng geclausuleerde ruimte aan de lidstaten tot het handhaven, respectievelijk vaststellen van regels die *afwijken* van richtlijnen die op grond van dat artikel zijn vastgesteld. Aangenomen moet worden dat die bevoegdheid zich ook uitstrekt ten aanzien van regels die op grond van de artt. 95 en 100A EG (oud) zijn vastgesteld. Van die bevoegdheid kan alleen in zeer uitzonderlijke gevallen gebruik worden gemaakt. Zie daarvoor de Handleiding Wetgeving en Europa (Ministerie van Justitie, 2009), blz. 123-124 en 190.

*3.1.2 Reikwijdte - functioneel*
De richtlijn biedt geen alomvattende regeling van het gegevensbeschermingsrecht op Europees niveau. De reikwijdte van de richtlijn is op verschillende wijzen beperkt.
Allereerst is de reikwijdte van de richtlijn beperkt tot *geheel of gedeeltelijk geautomatiseerde* verwerkingen van persoonsgegevens. Niet-geautomatiseerde verwerkingen vallen alleen onder de reikwijdte van de richtlijn voorzover zij in een *bestand* zijn opgenomen of zullen worden opgenomen (artikel 3, eerste lid, richtlijn).
Verder beoogt de richtlijn alleen bescherming te bieden aan de *persoonsgegevens van natuurlijke personen* (artikel 1, eerste lid, richtlijn). Hoewel rechtspersonen blijkens de jurisprudentie van het EHRM onder omstandigheden ook een zekere aanspraak kunnen hebben op bescherming van hun persoonsgegevens, biedt de richtlijn die bescherming niet. Hieruit volgt overigens dat persoonsgegevens verwerkt in de context van eenmansbedrijven of personenvennootschappen zonder rechtspersoonlijkheid wel onder de reikwijdte van de richtlijn vallen.
Verder is de richtlijn niet van toepassing op de verwerking van persoonsgegevens die plaatsvindt krachtens titel V EU (oud) (*gemeenschappelijk buitenlands en veiligheidsbeleid*) en titel VI EU (oud) (*politiële en justitiële samenwerking in strafzaken*) (zie artikel 3, tweede lid, eerste gedachtestreepje, richtlijn). De EU is wel bevoegd op die terreinen regelgevend op te treden. Hierbij moet worden bedacht dat het Verdrag van Lissabon een einde heeft gemaakt aan de pijlerstructuur van de Europese Unie. Dit kan consequenties hebben voor

de uitleg van de reikwijdte van richtlijn door de Europese instellingen.
Vervolgens is de richtlijn niet van toepassing op alle verwerkingen van persoonsgegevens die betrekking hebben op *openbare veiligheid, defensie, staatsveiligheid en de activiteiten van de staat op strafrechtelijk gebied* (zie artikel 3, tweede lid, eerste gedachtestreepje, richtlijn). Op deze terreinen hebben de lidstaten hun eigen regelgevende bevoegdheden geheel of gedeeltelijk behouden.
Tenslotte heeft de richtlijn geen betrekking op de verwerking van persoonsgegevens door natuurlijke personen met uitsluitend *persoonlijke of huishoudelijke doeleinden* (artikel 3, tweede lid, tweede gedachtestreepje, richtlijn).

*3.1.3 Reikwijdte - territoriaal*
De regels voor de doorgifte van gegevens uit landen behorende tot de EU naar derde landen gelden ook voor gegevens uit landen die behoren tot de EER naar derde landen. Zie *Besluit van het Gemengd Comité van de EER nr. 83/1999 van 25 juni 1999 tot wijziging van Protocol nr. 37 en bijlage XI (Telecommunicatiediensten) bij de EER-Overeenkomst (PbEG 2000 L 296)*.

*3.1.4 Beginselen*
Aan de richtlijn liggen een aantal beginselen ten grondslag die ook hun weerslag vinden in de Wet bescherming persoonsgegevens en de andere wetgeving op het gebied van de gegevensbescherming.

*3.1.4.1 Doelbinding*
Persoonsgegevens worden alleen verwerkt ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Hieraan gekoppeld zijn verplichtingen tot dataminimalisatie, zorg voor de kwaliteit van gegevens, terughoudendheid met verdere verwerking en een beveiligingsverplichting (artikel 6 richtlijn).

*3.1.4.2 Non-discriminatie*
De verwerking van persoonsgegevens met een gevoelig karakter (godsdienst en levensovertuiging, politieke gezindheid, ras of etnische afkomst, lidmaatschap van een vakbond, gegevens betreffende de gezondheid en het seksuele leven en strafrechtelijke persoonsgegevens) is in beginsel verboden teneinde discriminatie als gevolg van de verspreiding van deze gegevens te voorkomen (artikel 8 richtlijn).

*3.1.4.3 Transparantie*
Verantwoordelijken moeten zoveel mogelijk transparantie betrachten ten aanzien van verwerkingen onder hun verantwoordelijkheid. Er is een meldplicht voor verwerkingen, hetzij bij de nationale toezichthouder (in Nederland het College bescherming persoonsgegevens, hetzij een eigen functionaris voor de gegevensbescherming.
Verantwoordelijken voor gegevensverwerkingen moeten aan betrokkenen bekend maken voor welke doeleinden zij gegevens verwerken. Er is ook een informatieplicht voor betrokkenen (artikelen 10 en 11 richtlijn).

*3.1.4.4 Zelfregulering*
Door middel van de vaststelling van een *gedragscode* (artikel 27 richtlijn) en de aanstelling van een *functionaris voor de gegevensbescherming* (artikel 18 richtlijn) kunnen organisaties de normen voor gegevensbescherming beter toesnijden op de eigen aard van de sector en kunnen zij het toezicht op de naleving deels intern organiseren.

*3.1.4.5 Rechten van de betrokkene*
Betrokkenen hebben het recht op inzage, correctie, afscherming, uitwissing en verzet van de hen betreffende gegevens (artikel 12 tot en met 15 richtlijn).

*3.1.4.6 Positie derde landen*
De EU vormt één ruimte waarbinnen een vrij verkeer van persoonsgegevens, beschermd door de waarborgen die de richtlijn biedt, mogelijk is. Verkeer van persoonsgegevens vanuit de lidstaten met derde landen is niet onbeperkt mogelijk wanneer in die derde landen geen passend niveau van gegevensbescherming bestaat (artikel 25 en 26 richtlijn).

*3.1.4.7 Onafhankelijk toezicht*
De lidstaten zijn verplicht zorg te dragen voor een onafhankelijk toezichthouder die doeltreffend moet kunnen optreden (artikel 28 richtlijn). De toezichthouder moet ook worden belast met *wetgevingsadvisering*. In Nederland wordt deze rol vervuld door het *College bescherming persoonsgegevens*.

## *3.2 Richtlijn nr. 2002/58/EG*

Het is van meet af aan de bedoeling geweest dat de richtlijn ook op het niveau van het Unierecht zou worden aangevuld met sectorale bepalingen. Zie overweging 68 van de richtlijn die naar dit uitgangspunt verwijst. In aanvulling op richtlijn nr. 95/46/EG heeft de EU één sectorale richtlijn vastgesteld. Het gegevensbeschermingsregime voor de telecommunicatiesector is neergelegd in *richtlijn nr. 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PbEG L 201)*. Deze richtlijn is in Nederland geïmplementeerd in de hoofdstukken 11 en 13 van de *Telecommunicatiewet*. De richtlijn is, anders dan richtlijn nr. 95/46/EG, voorwerp van regelmatige wijziging. Mogelijk valt dat te verklaren uit de grotere techniekafhankelijkheid van deze regelgeving.
Grondslag en doelstellingen van richtlijn nr. 2002/58/EG stemmen overeen met die van richtlijn nr. 95/46/EG, met dien verstande dat de doelstellingen specifiek zijn toegesneden op de aard van de telecommunicatiesector. De begripsbepalingen van richtlijn nr. 95/46/EG zijn van toepassing op hetgeen geregeld is in richtlijn nr. 2002/58/EG. Ook overigens wordt in richtlijn nr. 2002/58/EG veelvuldig verwezen naar richtlijn nr. 95/46/EG.

Gelet op het sectorgebonden karakter van richtlijn nr. 2002/58/EG en het daardoor specifieke karakter van de bijbehorende implementatiewetgeving wordt op deze richtlijn niet verder ingegaan.

## *3.3 Kaderbesluit nr. 2008/977/JBZ*

Hierboven is uiteengezet dat richtlijn nr. 95/46/EG vastgesteld is met het oog op versterking van de interne markt. Verder heeft de richtlijn geen betrekking op gegevensverwerkingen die niet binnen de sfeer van het vroegere Gemeenschapsrecht vallen, waaronder in elk geval begrepen verwerkingen die plaatsvinden onder titel VI EU (oud). Verder is de richtlijn niet van toepassing op de gegevensverwerkingen ten behoeve van de nationale veiligheid en activiteiten van de staat op strafrechtelijk gebied.
Wat gegevensbescherming in het kader van titel VI EU (oud) betreft, heeft de EU in de vorm van *kaderbesluit nr. 2008/977/JBZ van de Raad van de Europese Unie van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (PbEU L 350)* een afzonderlijk gegevensbeschermingsregime vastgesteld voor de samenwerking tussen de politie- en justitieautoriteiten van de lidstaten. De grondslag voor het kaderbesluit wordt gevormd door de artikelen 30, 31 en 34, tweede lid, onder b, van het EU (oud). Het gegevensbeschermingsregime van het kaderbesluit is beperkt. Het heeft uitsluitend betrekking op de onderlinge samenwerking van bevoegde autoriteiten van de lidstaten. Het heeft geen betrekking op bescherming van persoonsgegevens die in het kader van de uitoefening van de politietaak, of als strafvorderlijk gegeven op nationaal niveau in Nederland worden verwerkt.
Inhoudelijk wijkt dit gegevensbeschermingsregime op belangrijke onderdelen af van dat van richtlijn nr. 95/46/EG. Hierop wordt in het kader van deze leidraad niet nader ingegaan, vanwege het specifieke karakter van het kaderbesluit.
Het kaderbesluit moet nog worden geïmplementeerd. Daarvoor zal wijziging van de Wet politiegegevens en van de Wet justitiële en strafvorderlijke gegevens moeten plaatsvinden.

## *3.4 Overig Europees dataprotectierecht*

Andere sectorale richtlijnen dan richtlijn nr. 2002/58/EG zijn nooit totstandgekomen. Wel wordt in andere richtlijnen regelmatig, soms impliciet, soms expliciet, verwezen naar richtlijn nr. 95/46/EG of richtlijn nr. 2002/58/EG.

Voorbeelden

Artikel 10 van richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L 144) en artikel 10 van richtlijn nr. 2002/65/EG van het Europees Parlement en de Raad van 23 september 2002 betreffende de verkoop op afstand van financiële diensten aan consumenten (PbEG L 271) stemmen vrijwel letterlijk overeen met artikel 13 van richtlijn nr. 2002/58/EG.
Zie artikel 9 van richtlijn nr. 2005/44/EG van het Europees Parlement en de Raad van de Europese Unie van 7 september 2005 betreffende geharmoniseerde River Information Services (RIS) op de binnenwateren in de Gemeenschap (PbEG L 255) voor een voorbeeld van een expliciete verwijzing.

Op EU-niveau bestaan nog verschillende gegevensbeschermingsregimes voor specifieke toepassingen. Te denken valt aan het de regimes voor het Schengen Information System II, het Customs Information System, het Europolbesluit, de verdragen tussen de EU en derde landen als de Verenigde Staten en Australië over de overdracht van passagiersgegevens. Ook op deze instrumenten gaat deze leidraad niet in.

# 4. Plaats van de Wbp in de Nederlandse wetgeving

## *4.1 Implementatie richtlijn nr. 95/46/EG*

De Wbp is de regeling waarin richtlijn nr. 95/46/EG primair is geïmplementeerd. De richtlijn is daarnaast ook in enkele bijzondere wettelijke regelingen geïmplementeerd, de Kieswet en de Wet gemeentelijke basisadministratie persoonsgegevens. Daarop wordt in paragraaf 4.5 teruggekomen. Het karakter van de Wbp als implementatieregeling brengt met zich dat aan de Wbp een bijzondere betekenis toekomt. Wanneer wordt overwogen een wettelijk voorschrift te ontwerpen dat aspecten van de bescherming van persoonsgegevens regelt die onder het bereik van de richtlijn vallen, dient eerst te worden nagegaan of de Wbp het desbetreffende onderwerp niet reeds regelt. De ervaring leert dat dit, gegeven het algemeen-abstracte karakter van de normen van de richtlijn en de Wbp, niet altijd onmiddellijk duidelijk is. Neem daarover zonodig contact op met de directie Wetgeving van het Ministerie van Justitie. Afwijken van de Wbp brengt al snel het risico van handelen in strijd met richtlijn nr. 95/46/EG met zich. Dit moet worden vermeden. Het Ministerie van Justitie is bij de wetgevingstoetsing uiterst terughoudend met het aanvaarden van afwijkingen van de Wbp.

Advies

Neem contact op met de directie Wetgeving van het Ministerie van Justitie indien niet op voorhand duidelijk is of een voorgenomen wettelijke regeling die aspecten van bescherming van persoonsgegevens regelt, niet reeds geheel of gedeeltelijk wordt geregeld in de Wbp.

## *4.2 Nadere invulling grondrecht op bescherming van de persoonlijke levenssfeer*

Hierboven is al ingegaan op de omstandigheid dat in de Wbp uitvoering is gegeven aan artikel 10, tweede en derde lid, van de Grondwet. Ook in dat opzicht is de Wbp dus geen regeling met een betrekkelijk willekeurig karakter.

## 4.3 Aard van de normering van de Wbp, publiek- en privaatrecht

De begripsbepalingen, de reikwijdtebepalingen en de materiële normen van de Wbp zijn, een enkele uitzondering daargelaten, zonder onderscheid van toepassing in rechtsverhoudingen die door het bestuursrecht én in rechtsverhoudingen die door het privaatrecht worden beheerst. Voor de regeling van de rechtsbescherming heeft de wetgever wel aansluiting gezocht aan het bestaande onderscheid tussen het bestuursrecht en het privaatrecht. Indien beslissingen op verzoeken van betrokkenen om inzage of correctie, dan wel een reactie op de uitoefening van het recht op verzet jegens een verantwoordelijke, afkomstig zijn van een verantwoordelijke die als bestuursorgaan moet worden aangemerkt, geldt de Awb. Voor alle andere gevallen staat een bijzondere verzoekschriftprocedure bij de burgerlijke rechter open.
Toch wordt de Wbp doorgaans als een bestuursrechtelijke wet aangemerkt. Reden daarvoor is dat de Wbp voorziet in specifiek bestuursrechtelijk toezicht, gecombineerd met de mogelijkheid om bestuursrechtelijke sancties op te leggen. Rechtsbescherming tegen besluiten houdende een sanctieoplegging wordt geboden door de bestuursrechter.

## 4.4 Begripsbepalingen van de Wbp

*4.4.1 Algemeen*
Een aantal begripsbepalingen van de Wbp worden hier expliciet behandeld. Deze begripsbepalingen hebben niet alleen betekenis in het verband van de Wbp, maar ook in andere wetgeving. In de andere specifieke gegevensbeschermingswetten, *de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2002*, worden dezelfde begrippen gebruikt. Wanneer het noodzakelijk is in specifieke wetgeving bepalingen met betrekking tot de verwerking van persoonsgegevens op te nemen, dient dit in beginsel alleen te geschieden door gebruik te maken van het begrippenapparaat van de Wbp. Daarbij moet uitsluitend naar de Wbp worden verwezen, bij voorkeur op onderstaande wijze. Het opstellen van afwijkende begripsbepalingen zijn afwijkingen van de Wbp zelf, en bovendien - in veel gevallen - afwijkingen van richtlijn nr. 95/46/EG. Afwijking van de Wbp kan alleen indien daarvoor een dringende noodzaak aanwezig is en er overleg heeft plaatsgevonden met de directie Wetgeving van het Ministerie van Justitie. Afwijking van de richtlijn is, tenzij dit gerechtvaardigd is op grond van primair of secundair Unierecht, uitgesloten.

Advies

Wanneer de noodzaak vaststaat om in een voorgenomen wettelijke regeling aspecten van de verwerking van persoonsgegevens of van de bescherming van persoonsgegevens op te nemen, wordt daarbij gebruik gemaakt van de in artikel 1 van de Wbp gedefinieerde begrippen, met gebruikmaking van onderstaande modelbepaling.
Over de noodzaak om in een voorgenomen wettelijke regeling met betrekking tot de bescherming van persoonsgegevens van de Wbp of van richtlijn nr. 95/46/EG afwijkende begrippen op te nemen wordt voorafgaand overleg gepleegd met de directie Wetgeving van het Ministerie van Justitie.

Modelbepaling

*In deze wet (en de daarop berustende bepalingen) wordt verstaan onder: persoonsgegevens, verwerking van persoonsgegevens, bestand, verantwoordelijke, bewerker, onderscheidenlijk betrokkene, hetgeen daaronder wordt verstaan in artikel 1 van de Wet bescherming persoonsgegevens.*

Voorbeeld

Artikel 1, onder o, van de Scheepvaartverkeerswet

Bij het ontwerpen van een regeling met aspecten van bescherming van persoonsgegevens wordt, met inachtneming van het bovenstaande, gebruik gemaakt van de onderstaande begrippen uit de Wbp.

*4.4.2 Persoonsgegeven - positie natuurlijke personen en rechtspersonen*
Onder "persoonsgegeven" wordt verstaan: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1, onder a, Wbp). Het begrip persoonsgegeven moet ruim worden opgevat. Het gaat zeker niet alleen om basale gegevens als naam, adres en woonplaats, maar om elk gegeven dat in verband kan worden gebracht met een (identificeerbare) natuurlijke persoon. Een pasfoto, een vingerafdruk, een voertuigkenteken, een telefoonnummer, en een e-mailadres zijn alle voorbeelden van persoonsgegevens.
Verder is van belang dat de bescherming van persoonsgegevens alleen betrekking heeft op de bescherming van de gegevens van *natuurlijke personen*. Rechtspersonen kunnen dus op grond van de Wbp geen aanspraak maken op bescherming van de hun betreffende gegevens. Een zekere bescherming van hun gegevens kunnen rechtspersonen overigens wel ontlenen aan de *Handelsregisterwet 2007* en de *Wet documentatie vennootschappen*. Laatstgenoemde wet wordt op korte termijn vervangen door de *Wet controle op rechtspersonen*. Op grond van de *Wet justitiële en strafvorderlijke gegevens* kan ten aanzien van een rechtspersoon een verklaring omtrent het gedrag worden verleend.
Wel moet worden bedacht dat in verband met de belangrijke plaats die rechtspersonen in de rechtsorde innemen, de verwerking van persoonsgegevens van natuurlijke personen

*in verband met rechtspersonen* veelvuldig voorkomt. Te denken valt aan verwerking van persoonsgegevens van bestuurders van rechtspersonen in openbare registers als het handelsregister, of de verwerking van persoonsgegevens op grond van de *Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (BIBOB)*.
Verder impliceert de beperking van de reikwijdte van de Wbp tot natuurlijke personen dat de gegevens betreffende eenmansbedrijven, maatschappen of andere personenvennootschappen in de regel worden beschermd door de Wbp. Daarmee moet rekening worden gehouden bij de voorbereiding van wetgeving die geheel of gedeeltelijk is gericht tot dit type onderneming.

Voorbeeld

Zie de memorie van toelichting bij het voorstel van wet houdende *wijziging van de Scheepvaartverkeerswet in verband met de implementatie van richtlijn nr. 2005/44/EG van het Europees Parlement en de Raad van de Europese Unie van 7 september 2005 betreffende geharmoniseerde River Information Services (RIS) op de binnenwateren in de Gemeenschap (PbEU L 255)* (Kamerstukken II 2006/07, 30 974, nr. 3), waarin aandacht wordt gegeven aan de verwerking van locatiegegevens van binnenschepen.

*4.4.3 Verwerking van persoonsgegevens*
Onder "verwerking van persoonsgegevens" wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (art. 1, onder b, Wbp). Ook deze begripsbepaling is zeer breed en overigens niet limitatief geformuleerd. Verwerken omvat alle denkbare handelingen die met betrekking tot persoonsgegevens kunnen worden verricht.

*4.4.4 Bestand*
Een "bestand" omvat: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen (art. 1, onder c, Wbp). Het begrip bestand is vooral van betekenis bij de bepaling van de reikwijdte van de Wbp. De Wbp is met name bedoeld om de gevolgen van de geautomatiseerde verwerking van persoonsgegevens te regelen, maar de wet strekt zich ook uit tot de niet geautomatiseerde (papieren) verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

*4.4.5 Verantwoordelijke*

De wet omschrijft "verantwoordelijke" als: de natuurlijke persoon, de rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met andere, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (art. 1, onder d, Wbp). De verantwoordelijke is degene op wie, krachtens de Wbp, een aantal belangrijke verplichtingen rusten (vgl. art. 15 Wbp). Voornaamste verplichting is dat de verantwoordelijke de doeleinden van de gegevensverwerking moet vaststellen, een en ander voor zover de wetgever in een afzonderlijk geval de doeleinden van de gegevensverwerking niet zelf bepaalt. Verwerking van persoonsgegevens mag alleen in het kader van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde plaatsvinden. De doeleinden van gegevensverwerking dienen door de verantwoordelijke bij wijze van melding openbaar te worden gemaakt. In verband daarmee dient de identiteit van de verantwoordelijke duidelijk te zijn. Op de verantwoordelijke rust verder een meldplicht. De verantwoordelijke is voorts degene die door de betrokkene moet worden aangesproken voor de uitoefening van de aan hem door de Wbp toegekende rechten. Belangrijk in dit verband is dat vaststelling van het doel van gegevensverwerking, én aanwijzing van een verantwoordelijke ook *door de wetgever* kan plaatsvinden. Wordt die keuze gemaakt, dan moet gebruik worden gemaakt van onderstaande modelbepaling.

Modelbepaling

*Ten behoeve van (opsomming doeleinden of verwijzing naar een andere bepaling waarin de doeleinden zijn beschreven) worden persoonsgegevens verwerkt. (Bestuursorgaan) is verantwoordelijke voor deze verwerking.*

Toelichting

Deze modelbepaling kan worden gebruikt in aanvulling op de in de paragraaf 4.4.1 behandelde model, waarmee voor de begrippen uit de Wbp door middel van verwijzing wordt aangesloten aan het begrippenapparaat van de Wbp.

Voorbeelden

Artikel 3 van de Wet gemeentelijke basisadministratie persoonsgegevens
Artikel 3a eerste lid, van de Kadasterwet
Artikel 4 van de Wet kenbaarheid publiekrechtelijke beperkingen onroerende zaken
Artikel 14 van de Wet ter voorkoming van witwassen en financieren van terrorisme
Artikel 2 van de Wet justitiële en strafvorderlijke gegevens
Artikel 9a van de Wet verzelfstandiging informatiseringsbank

Dit zijn bestaande voorbeelden van wettelijke doelomschrijvingen veelal gecombineerd met de aanwijzing van een verantwoordelijke. Deze bepalingen konden (uiteraard) nog niet met gebruikmaking van de modelbepalingen totstandkomen.

*4.4.6 Gedeelde verantwoordelijkheid*
Onder omstandigheden kan het noodzakelijk zijn in een wetsvoorstel meer dan één verantwoordelijke aan te wijzen voor een verwerking. Dat doet zich met name voor wanneer er sprake is van verwerkingen die op rijksniveau zijn ingesteld, maar op decentraal niveau (bijvoorbeeld door burgemeester en wethouders) moeten worden bijgehouden. In die gevallen moet de onderlinge afgrenzing van de (deel)verantwoordelijkheid nauwkeurig worden geregeld. Dat is noodzakelijk, omdat de wetgever de betrokkene niet in het ongewisse mag laten over de vraag tot wie hij zich moet wenden voor de uitoefening van zijn rechten.

Voorbeeld

Artikel 2e van de Wet op de jeugdzorg biedt een voorbeeld van gedeelde verantwoordelijkheid voor gegevensverwerking. Het betreft hier de verwijsindex risico's jeugdigen.

*4.4.7 Bewerker*
De "bewerker" is: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (art. 1, onder e, Wbp). In veel gevallen vindt de verwerking van persoonsgegevens plaats in opdracht van de verantwoordelijke, door een derde partij. De Wbp stelt daaraan de eis dat dit geschiedt krachtens een bewerkersovereenkomst (art. 14, tweede lid, Wbp). De Wbp vult overigens de rechtsbetrekking tussen verantwoordelijke en bewerker nader in (artt. 12 tem 14 Wbp).

*4.4.8 Betrokkene*
De "betrokkene" is degene op wie een persoonsgegeven betrekking heeft (art. 1, onder f, Wbp). Aan de betrokkene zijn, ter bescherming van zijn gegevens, door de wetgever een aantal belangrijke rechten toegekend: het recht van inzage (art. 35 Wbp), het recht van correctie (art. 36 Wbp) en het recht van verzet (art. 40 Wbp). Beide eerstgenoemde rechten zijn ook constitutioneel van aard (art. 10, derde lid, van de Grondwet). Voorts kent de Wbp enkele bijzondere bepalingen met betrekking tot rechtsbescherming en schadevergoeding (hoofdstuk 8 Wbp). Die bepalingen zijn weliswaar gericht tot belanghebbenden, maar in veel gevallen zal een belanghebbende in zijn hoedanigheid van betrokkene een beroep doen op die bepalingen.

## 4.5 Reikwijdte van de Wbp

Hoewel de Wbp in beginsel van toepassing is op alle vormen van verwerking van persoonsgegevens, gelden er een aantal belangrijke uitzonderingen op dit uitgangspunt. Die uitzonderingen zijn in de meeste gevallen terug te voeren op de reikwijdtebepaling van de richtlijn. In enkele andere gevallen vloeit dat voort uit de structuur van de Nederlandse regelgeving.

*4.5.1 Beperking van de reikwijdte van de Wbp voortvloeiend uit richtlijn nr. 95/46/EG: openbare veiligheid, defensie, veiligheid van de staat, activiteiten van de staat op strafrechtelijk gebied*
Artikel 3, tweede lid, eerste gedachtestreepje, van de richtlijn zondert van de reikwijdte van de richtlijn alle verwerkingen van persoonsgegevens uit die met het oog op de uitoefening van niet binnen het (vroegere) Gemeenschapsrecht vallende activiteiten worden verricht. De richtlijn geeft daarbij aan dat het activiteiten betreft zoals bedoeld in de titels V en VI EU (oud), en noemt daarbij de in het kopje genoemde activiteiten. De opsomming is niet limitatief. Uit de uitspraak van het HvJEG van 30 mei 2006 nrs. C-317/04 en C-318/04 (Europees Parlement/Raad en Europees Parlement/Commissie) blijkt in ieder geval dat de overdracht van passagiersgegevens aan buitenlandse autoriteiten belast met strafrechtelijke taken, buiten de werkingssfeer van de richtlijn ligt, ook al werden de gegevens door luchtvaartmaatschappijen voor eigen doeleinden verzameld. Bedacht moet worden dat ook na het Verdrag van Lissabon artikel 3, tweede lid, eerste gedachtestreepje, van de richtlijn betrekking blijft hebben op enkele terreinen waarvoor de EU niet tot regelgeving bevoegd is. Voor de Wbp heeft dit tot consequentie dat de Wbp niet van toepassing is op de navolgende verwerkingen.

*4.5.1.1 Wet op de inlichtingen- en veiligheidsdiensten 2002*
De Wbp is niet van toepassing op de verwerking en bescherming van persoonsgegevens door of ten behoeve van de *inlichtingen- en veiligheidsdiensten*, bedoeld in de *Wet op de inlichtingen- en veiligheidsdiensten 2002* (art. 2, tweede lid, onder b, Wbp).

*4.5.1.2 Politietaken*
De Wbp is niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de *politietaak*, bedoeld in de artikelen 2 en 6, eerste lid, van de Politiewet 1993 (art. 2, tweede lid, onder c, Wbp). Zie verder paragraaf 7.4.2.

*4.5.1.3 Wet justitiële en strafvorderlijke gegevens*
De Wbp is niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de *Wet justitiële en strafvorderlijke gegevens* (art. 2, tweede lid, onder e, Wbp). Zie verder paragraaf 7.4.1.

*4.5.1.4 Krijgsmacht*
De Wbp is niet van toepassing op de verwerking van persoonsgegevens door de *krijgsmacht*. Deze exceptie is niet algemeen geformuleerd. Zij vindt alleen toepassing in afzonderlijke gevallen van inzet of beschikbaarstelling van de krijgsmacht wanneer de Minister van Defensie daartoe beslist (art. 2, derde lid, Wbp).

*4.5.1.5 Persoonlijke of huishoudelijke doeleinden*
Artikel 3, tweede lid, tweede gedachtestreepje, van de richtlijn zondert van de reikwijdte van de richtlijn de verwerking van persoonsgegevens uit die door een natuurlijk persoon ten behoeve van uitsluitend *persoonlijke of huishoudelijke doeleinden* worden verricht (art. 2, tweede lid, onder a, Wbp). Deze exceptie moet als gevolg van het arrest van het HvJEG van 6 november 2003, nr. C-101/01 (Lindqvist), beperkt worden uitgelegd. Indien er sprake is van een verwerking die op internet is geplaatst, kan deze exceptie niet worden ingeroepen.

*4.5.1.6 Activiteiten van de staat op strafrechtelijk gebied*
De in de richtlijn genoemde exceptie *activiteiten van de staat op strafrechtelijk gebied* verdient afzonderlijke aandacht. Hoewel de Wbp slechts expliciet verwijst naar de Politiewet 1993 en de Wet justitiële en strafvorderlijke gegevens, lijkt de interpretatie gerechtvaardigd dat deze exceptie ook de verwerking van persoonsgegevens omvat die voortvloeit uit de volgende regelingen: *Wetboek van Strafvordering, Wet politiegegevens, Penitentiaire beginselenwet en de Beginselenwet verpleging ter beschikking gestelden.* Volledigheidshalve wordt nog vermeld dat strafrechtelijke persoonsgegevens overigens vallen onder het regime van de bijzondere persoonsgegevens. De exceptie van de richtlijn heeft geen betrekking op de activiteiten van particuliere bewakingsdiensten of privé-detectives. Deze activiteiten worden immers niet door de staat verricht. Evenmin ziet de exceptie op de omgang met strafrechtelijke persoonsgegevens door particulieren.

*4.5.2 Beperking van de reikwijdte van de Wbp als gevolg van nationale wetgeving*
Niet uit de richtlijn voortvloeiende excepties op de reikwijdte van de Wbp betreffen twee afzonderlijke wetten: *de Wet gemeentelijke basisadministratie persoonsgegevens* en de *Kieswet* (artikel 2, tweede lid, onder d en f, Wbp). Beide wetten vallen dus volledig onder de werking van de richtlijn.

*4.5.3 Vrijheid van meningsuiting*
Een gedeeltelijke uitzondering op de reikwijdte van de Wbp geldt voor de verwerking van persoonsgegevens ten behoeve van doeleinden die kunnen worden samengevat onder de noemer *vrijheid van meningsuiting* (artikel 3 Wbp).

*4.5.4 Territoriale reikwijdte Wbp*
De reikwijdte van de Wbp is in territoriaal opzicht beperkt tot de verwerking van persoonsgegevens door verantwoordelijken die in Nederland over een vestiging beschikken. Bevindt de verantwoordelijke zich buiten de Europese Unie en maakt hij gebruik van al

dan niet geautomatiseerde middelen die zich in Nederland bevinden, dan dient hij een persoon of instantie aan te wijzen in Nederland die namens hem handelt overeenkomstig de bepalingen van de Wbp (art. 4 Wbp). De achtergrond hiervan is dat de Europese Unie één ruimte vormt waarbinnen een vrij verkeer van persoonsgegevens kan plaatsvinden, mits dit gebeurt in overeenstemming met richtlijn nr. 95/46/EG. Aanwijzing van een verantwoordelijke is daarvoor noodzakelijk. Plaats en land van vestiging van de verantwoordelijke zijn bepalend voor de bevoegdheid van de toezichthouder. De bevoegdheid van de toezichthouders om handhavingsbesluiten te nemen is een zaak van nationaal recht. Het is onder de Wbp overigens mogelijk dat de toezichthouder (het Cbp) optreedt ten behoeve van de handhaving van het gegevensbeschermingsrecht van een andere EU-lidstaat (art. 51, eerste lid, Wbp).

*4.5.5 Wet bescherming persoonsgegevens BES*

De komende staatkundige hervorming van het Koninkrijk der Nederlanden heeft ook consequenties voor de bescherming van persoonsgegevens. De eilandgebieden Bonaire, Sint Eustatius en Saba (de BES-eilanden) zullen tot het grondgebied van Nederland gaan behoren. De BES-eilanden behouden vooralsnog hun LGO-status (Landen en Gebieden Overzee) in de zin van het Vierde Deel van het VWEU (art. 198 e.v. VWEU). Daaruit volgt dat richtlijn nr. 95/46/EG vooralsnog niet van toepassing is op de verwerking van persoonsgegevens door verantwoordelijken gevestigd op de BES-eilanden. Wel is het zo dat artikel 10 van de Grondwet in volle omvang op de BES-eilanden gaat gelden. Dat betekent dat het recht op bescherming van de persoonlijke levenssfeer beschermd zal worden, en dat ook de wetgever de regelingsopdrachten van artikel 10, tweede en derde lid, van de Grondwet ten aanzien van de BES-eilanden moet gaan uitvoeren. Aangezien onder Nederlands-Antilliaans recht nooit een algemene regeling voor gegevensbescherming tot stand is gekomen die krachtens de Invoeringswet BES op de BES-eilanden zou kunnen gaan gelden, moet hetzij de Wbp, hetzij een afzonderlijke regeling voor de bescherming van persoonsgegevens op de BES-eilanden gaan gelden. Gelet op de sociale structuur van de BES-eilanden, de beperkte bestuurlijke capaciteit van de eilandsoverheden en relatieve ingewikkeldheid van de Wbp, heeft de wetgever vooralsnog gekozen voor een - in vergelijking met Nederland - sterk afgeslankte regeling van de bescherming van persoonsgegevens. Het voorstel voor een *Wet bescherming persoonsgegevens BES* (Kamerstukken II 2009/10, 32 161, nr. 2) voorziet daarin. De Wbp BES kent geen regeling voor gedragscodes, meldplichten en voorafgaande onderzoeken.

Er zal wel worden voorzien in onafhankelijk toezicht, zodat Nederland, ook wat de BES-eilanden betreft, in ieder geval voldoet aan de eisen die voortvloeien uit het Dataprotectieverdrag, met inbegrip van het Aanvullend Protocol. Zie daarover nader paragraaf 2.4.

## 4.6 De Wbp als algemene voorziening - afwijkingen en aanvullingen van de Wbp

Met inachtneming van hetgeen hierboven is behandeld ten aanzien van de reikwijdte van de Wbp en met inachtneming van de bestaande bijzondere wetgeving, fungeert de Wbp als de algemene voorziening voor het gegevensbeschermingsrecht in Nederland. De Wbp moet daarom worden aangemerkt als een algemene wet in de zin van aanwijzing 49 van de Aanwijzingen voor de regelgeving. Van de Wbp wordt ook daarom alleen afgeweken als dat echt noodzakelijk is. De redenen voor de *afwijking* worden in de memorie van toelichting gemotiveerd. Over afwijkingen van de Wbp vindt tevoren *overleg plaats met de directie Wetgeving van het Ministerie van Justitie*.
Voor *aanvulling* van de Wbp met sectorale normen bestaan ruimere mogelijkheden. Dat volgt uit het stelsel van richtlijn nr. 95/46/EG. Zie in dit verband nader paragraaf 3.2. Artikel 5 van richtlijn nr. 95/46/EG geeft de lidstaten daartoe een zekere vrijheid. Er bestaan in de wetgeving diverse voorbeelden van wetten die de Wbp aanvullen. Dergelijke regeling gelden naast en niet in plaats van de Wbp.

Voorbeelden

Hoofdstuk 11 van de Telecommunicatiewet (telecommunicatiesector)
Artikelen 454 tot en met 459 van titel 7 van Boek 7 van het Burgerlijk Wetboek (zorgsector).

Op grond van artikel 25 van de Wbp zijn voorts een aantal *gedragscodes* vastgesteld die gelden voor een aantal sectoren van het bedrijfsleven. Gedragscodes worden geacht een nadere invulling van de Wbp te zijn voor de desbetreffende sector van het bedrijfsleven. Het Cbp kan op aanvraag van de sector bij besluit een uitspraak doen over de representativiteit van een gedragscode. Er zijn tot dusverre acht gedragscodes vastgesteld.

## 4.7 De Wbp en het legaliteitsbeginsel

Het algemene karakter van de Wbp komt ook tot uitdrukking in de omstandigheid dat de Wbp regelt dat van een aantal materiële normen uitsluitend kan worden afgeweken indien daarvoor een formeelwettelijke grondslag bestaat. Bij het ontwerpen van wetgeving met aspecten van gegevensbescherming verdient dit dan ook bijzondere aandacht. Het betreft de volgende normen.

*4.7.1 Verwerking in overeenstemming met de wet*
Art. 6 Wbp formuleert de algemene norm dat persoonsgegevens slechts *"in overeenstemming met de wet* en op behoorlijke en zorgvuldige wijze worden verwerkt". Deze norm impliceert in ieder geval dat buitenwettelijke verwerking van persoonsgegevens in algemene zin niet toelaatbaar is. Overigens verwijst deze norm naar de algemene beginselen van behoorlijk bestuur uit het bestuursrecht en de zorgvuldigheidsnorm uit het burgerlijk recht.

*4.7.2 Wettelijk verbod op verwerken bijzondere persoonsgegevens*
*Bijzondere persoonsgegevens* zijn persoonsgegevens met betrekking tot: godsdienst of levensovertuiging, ras (of etniciteit), politieke gezindheid, gezondheid, seksueel levensgedrag, en het lidmaatschap van een vakvereniging. Met bijzondere persoonsgegevens worden gelijkgesteld strafrechtelijke persoonsgegevens of gegevens betreffende onrechtmatig of hinderlijk gedrag naar aanleiding van een opgelegd verbod naar aanleiding van dat gedrag.
Ingevolge art. 16 Wbp is het verwerken van bijzondere persoonsgegevens *verboden*, behoudens een uitdrukkelijke regeling in de Wbp (of een van de Wbp afwijkende wet). Verder bevat art. 23 Wbp een opsomming van een aantal algemene uitzonderingen op het verwerkingsverbod.

*4.7.3 Doorbreken verbod op verwerking bijzondere persoonsgegevens alleen op wettelijke grondslag*
In de artikelen 17 tot en met 22 Wbp zijn de gevallen geregeld waarin een uitzondering op het verwerkingsverbod bestaat voor de verwerking van gegevens betreffende godsdienst of levensovertuiging (art. 17 Wbp), ras (art. 18 Wbp), politieke gezindheid (art. 19 Wbp), lidmaatschap van een vakbond (art. 20 Wbp), gezondheid (art. 21 Wbp) en strafrechtelijke persoonsgegevens (art. 22 Wbp). Het voert in het kader van deze leidraad te ver om de vele in deze artikelen begrepen gedetailleerde uitzonderingen te behandelen. Wanneer het noodzakelijk is bijzondere persoonsgegevens te verwerken voor de uitvoering van een wettelijke regeling dient daarom eerst te worden nagegaan of het verwerken van deze gegevens reeds toelaatbaar is krachtens de artt. 17 t/m 22 Wbp.

*4.7.4 Bijzondere uitzonderingen op het verwerkingsverbod*
Het verbod om bijzondere persoonsgegevens te verwerken kan alleen worden doorbroken indien dat uitdrukkelijk is geregeld in hoofdstuk 2, paragraaf 2, van de Wbp. Die paragraaf bevat een groot aantal uitzonderingen die zijn toegesneden op de diverse categorieën bijzondere persoonsgegevens (art. 17 tem 22 Wbp).

*4.7.5 Algemene uitzonderingen op het verwerkingsverbod*
Wanneer blijkt dat een voorgenomen regeling die voorziet in de verwerking van bijzondere persoonsgegevens niet kan worden gerechtvaardigd op grond van een van de gronden, opgenomen in de artikelen 17 tot en met 22 Wbp, dan moet worden nagegaan of de algemene uitzonderingen op het verwerkingsverbod van artikel 23 Wbp die ruimte wel bieden. De algemene uitzonderingen kunnen worden ingeroepen ten aanzien van alle typen bijzondere persoonsgegevens.

Algemene uitzonderingen zijn:
- uitdrukkelijke *toestemming* van de betrokkene (art. 23, eerste lid, onder a, Wbp)
- duidelijke *openbaarmaking* van de desbetreffende gegevens van en door de betrokkene (art. 23, eerste lid, onder b, Wbp)
- noodzaak in verband met de vaststelling, uitoefening of verdediging van een recht *in rechte* (art. 23, eerste lid, onder c, Wbp)
- het voldoen aan een *volkenrechtelijke verplichting* (art. 23, eerste lid, onder d, Wbp)
- art. 23, eerste lid, onder e, Wbp biedt de mogelijkheid om het verwerkingsverbod voor bijzondere persoonsgegevens te *doorbreken* indien dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit *bij wet* wordt bepaald, dan wel het College bescherming persoonsgegevens *ontheffing* heeft verleend.

Advies

De wetgevingspraktijk leert dat op de doorbreking van het wettelijk verbod, bedoeld in art. 23, eerste lid, onder e, Wbp regelmatig een beroep wordt gedaan. Daarom volgen hieronder enige richtlijnen en voorbeelden voor het gebruik van deze uitzondering.

Allereerst

- artikel 23, eerste lid, onder e, van de Wbp is een *uitzonderingsregeling*; met de toepassing daarvan wordt grote terughoudendheid betracht
- ga daarom eerst zorgvuldig na of de voorgenomen regeling niet reeds valt onder de reeds in de artikelen 17 tem 22 Wbp geregelde doorbrekingen van het verwerkingsverbod; *overleg daarover zonodig met de directie Wetgeving van het Ministerie van Justitie*

Vervolgens
- ga zorgvuldig na of de voorgenomen regeling niet reeds valt onder de in artikel 23, eerste lid, onder a tot en met d, Wbp geregelde gevallen
- zie voor de vereisten waaraan *toestemming* in de context van de Wbp (en dus ook in de context van art. 23, eerste lid, onder a, van de Wbp) moet voldoen: art. 1, onder i, Wbp
- een volkenrechtelijke verplichting wordt bij of krachtens verdrag of bindend besluit van een volkenrechtelijke organisatie vastgesteld, *een regel van (intern) buitenlands recht is geen volkenrechtelijke verplichting in de zin van art. 23, eerste lid, onder d, Wbp*
- indien het voorstel van wet houdende *wijziging van de Wet bescherming persoonsgegevens in verband met de uitvoering van de op 26 juli 2007 te Washington tot stand gekomen Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers door luchtvaartmaatschappijen aan het Ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), met briefwisseling en verklaring (Trb. 2007, 129) (Kamerstukken II 2008/09, 31 734, nr. 2)* tot wet wordt verheven zal het nieuwe art. 23a Wbp voorzien in een nieuwe uitzonderingsgrond die de overdracht van bijzondere persoonsgegevens mogelijk maakt indien het recht van een derde land

daartoe noodzaakt, ook dat kan alleen wanneer daarvoor een zwaarwegend algemeen belang bestaat en passende waarborgen voor de bescherming van de persoonlijke levenssfeer bestaan, maar bovendien is voorzien in een toereikende grondslag krachtens een verdrag of een bindend EU- of EG-besluit

Tenslotte

- wanneer blijkt dat de gewenste voorziening noodzaakt tot het opstellen van nieuwe wetgeving - al dan niet gecombineerd met de aanvraag van een ontheffing bij het College bescherming persoonsgegevens - voorzie dan eerst in een *grondige motivering* van het zwaarwegend algemeen belang en expliciteer welke passende waarborgen voor de bescherming van de persoonlijke levenssfeer worden geboden
- indien *aanvraag van een ontheffing* bij het College bescherming persoonsgegevens wordt overwogen dient daarbij te worden betrokken dat deze ontheffingen uitsluitend voor een beperkte periode worden verleend en dat ten genoege van het College moet worden aangetoond dat er een concreet voornemen bestaat tot legalisatie; naarmate het wetgevingsproces verder is gevorderd en het voornemen daardoor meer is geconcretiseerd, zal deze bewijslast gemakkelijker kunnen worden gedragen
- in het *wetsvoorstel* dienen tenminste expliciet te zijn geregeld: *doeleinde(n) van de voorgenomen gegevensverwerking, omvang van de gegevensverstrekking - zo veel mogelijk te relateren aan specifieke bijzondere persoonsgegevens -, identiteit van de verantwoordelijke, regeling van de verstrekking van gegevens en van de eventueel beoogde verdere verstrekking, mede in relatie tot bestaande wettelijke geheimhoudingsplichten, waarborgen voor de gegevensverstrekking*, (sub) delegatie is gelet op de tekst van art. 23, eerste lid, onder e, Wbp niet aanvaardbaar
- in de *memorie van toelichting* wordt een expliciete *motivering van het zwaarwegend algemeen belang* gegeven en worden de te treffen *waarborgen voor de bescherming van de persoonlijke levenssfeer* expliciet uiteengezet
- na afronding van het wetgevingsproces geldt een *notificatieverplichting* voor de betrokken Minister aan de Europese Commissie (art. 23, derde lid, Wbp)

Voorbeelden

Artikel 53, tweede lid, van de Wet op de jeugdzorg
Artikel 107a van de Vreemdelingenwet 2000
Wet van 5 juli 2006 tot wijziging van de Wet op het onderwijstoezicht onder meer in verband met de bevoegdheid van de vertrouwensinspecteurs om bijzondere persoonsgegevens te verwerken, Stb. 335 (Kamerstukken 30 460)
Algemene wet erkenning EG-beroepskwalificaties, Stb. 2007, 530 (Kamerstukken 31 059)

*4.7.6 Persoonsidentificerende nummers*

*Persoonsidentificerende nummers* zijn als zodanig door de Europese en Nederlandse wetgever niet aangemerkt als bijzondere persoonsgegevens. Niettemin worden deze nummers wel op gelijke wijze als bijzondere persoonsgegevens benaderd, waar het gaat om de wijze waarop de wetgever daarmee moet omgaan. Uit oogpunt van de doorwerking van het legaliteitsbeginsel in de Wbp verdient de wijze van omgang met persoonsidentificerende nummers daarom afzonderlijke aandacht.

Een bij de wet voorgeschreven persoonsidentificerend nummer mag slechts worden gebruikt voor de uitvoering van de betrokken wet dan wel voor doeleinden die *bij de wet* zijn bepaald (artikel 24, eerste lid, Wbp). Verschil met de regeling over de verwerking van bijzondere persoonsgegevens is echter dat ook *bij amvb* regels kunnen worden gesteld over het gebruik van een in die amvb aan te wijzen nummer. Uiteraard kunnen bij amvb alleen nummers worden aangewezen die reeds bij een wet in het leven zijn geroepen.

Het meest algemeen gebruikelijke persoonsidentificerende nummer is het burgerservicenummer (BSN). Dient zich de noodzaak aan om gebruik van een persoonsidentificerend nummer voor te schrijven, dan wordt in beginsel het BSN gebruikt. Bedenk hierbij dat het gebruik van het BSN reeds in algemene zin geregeld is in de *Wet algemene bepalingen burgerservicenummer*. Voor het gebruik van andere nummers dan het BSN, zoals het sofinummer, het onderwijsnummer of het strafrechtsketennummer blijft een aparte wettelijke grondslag nodig.

Voorbeelden

Wet algemene bepalingen burgerservicenummer (BSN)
Besluit gebruik sofi-nummer Wbp (sofinummer)
Wet van 6 december 2001 tot wijziging van enkele onderwijswetten in verband met enkele aanpassingen met betrekking tot persoonsgebonden nummers in het onderwijs, Stb. 681 (Kamerstukken 25 828) (onderwijsnummer)
Artikel 9b van de Wet verzelfstandiging informatiseringsbank (te vervangen door artikel 24c van de Wet op het onderwijstoezicht opgenomen in artikel III van het voorstel van wet tot intrekking van de Wet verzelfstandiging informatiseringsbank en wijziging van diverse wetten in verband met de oprichting van de Dienst Uitvoering Onderwijs (DUO) (Kamerstukken II 2008/09, 31 944, nr. 2) (onderwijsnummer)
Artikel 27b Wetboek van Strafvordering (strafrechtsketennummer)

*4.7.6.1 Besluit gebruik sofi-nummer Wbp*

Met de totstandkoming van het BSN is het belang van het oude sociaal-fiscale nummer (*sofi-nummer*) afgenomen. Niettemin kan gebruik van het sofi-nummer in een wettelijk voorschrift nog zinvol zijn. Het betreft dan vooral het gebruik van het nummer ten behoeve van de identificatie van personen die niet (eerder) in de gemeentelijke basisadministratie persoonsgegevens zijn opgenomen, maar ten aanzien van wie wel aanknopingspunten bestaan met de Nederlandse rechtsorde, bijvoorbeeld in de vorm van een arbeidsrelatie met een in Nederland gevestigde werkgever, of het zijn van belastingplich-

tige naar Nederlands fiscaal recht, zonder dat sprake is van het houden van hoofdverblijf in Nederland. De wettelijke grondslag voor het sofi-nummer is neergelegd in *artikel 47b van de Algemene wet inzake rijksbelastingen.* Gegeven deze grondslag volgt uit art. 24, tweede lid, Wbp dat het voorschrijven van het gebruik van dit nummer bij algemene maatregel van bestuur mag plaatsvinden. Dit gebeurt in beginsel niet in andere algemene maatregelen van bestuur dan het *Besluit gebruik sofi-nummer Wbp*. Dit besluit valt onder de verantwoordelijkheid van de Minister van Justitie. Indien nieuw gebruik van het sofi-nummer wordt overwogen, behoort daarom overleg met de directie Wetgeving van het Ministerie van Justitie plaats te vinden. De Minister van Justitie voert terzake een ruimhartig beleid.

Advies

Indien nieuw gebruik van het sofi-nummer wordt overwogen, vindt in verband met de daarvoor noodzakelijke aanpassing van het Besluit gebruik sofi-nummer Wbp voorafgaand overleg plaats met de directie Wetgeving van het Ministerie van Justitie.

## *4.8 Wetgeving basisregistraties*

De deels nog in opbouw zijnde wetgeving op het gebied van *basisregistraties* is geen gegevensbeschermingswetgeving in strikte zin. Niettemin bevat deze wetgeving wel verplichtingen voor bestuursorganen die voortvloeien uit richtlijn nr. 95/46/EG en, waar deze van toepassing is, de Wbp.
De diverse wetten voor de basisregistraties beogen vastlegging van bepaalde gegevens in een daartoe bestemde basisregistratie door een aangewezen bestuursorgaan, ten behoeve van herhaald gebruik door aangewezen bestuursorganen bij de uitvoering van hun publieke taken, met als doel dat burgers en bedrijven slechts eenmaal deze gegevens hoeven te verstrekken. Het aangewezen bestuursorgaan heeft de verplichting zorg te dragen voor de actualiteit en de kwaliteit van de gegevensbestanden. Voor alle andere bestuursorganen bestaat er een gebruiksplicht voor de in de basisregistratie opgenomen gegevens. Zie hiervoor de brief van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de voorzitter van de Tweede Kamer der Staten-Generaal van 30 augustus 2004 (Kamerstukken II 2003/04, 29 362 en 26 387, nr. 20) en de bij die brief aangeboden *Wetgevingsnota basisregistraties.*
Inmiddels zijn een aantal wetten tot stand gekomen.

Voorbeelden

Handelsregisterwet 2007 (basisregistratie bedrijven)
Wet basisregistratie kadaster en topografie (basisregistratie kaarten en percelen)
Wet basisregistratie adressen en gebouwen (basisregistratie adressen en gebouwen)
Artikel 9a van de Wet verzelfstandiging informatiseringsbank (basisregistratie onderwijs) (te vervangen door artikel 24b van de Wet op het onderwijstoezicht, opgenomen in artikel III van het voorstel van wet tot intrekking van de Wet verzelfstandiging informatiseringsbank en wijziging van diverse wetten in verband met de oprichting van de Dienst Uitvoering Onderwijs (DUO) (Kamerstukken II 2008/09, 31 944, nr. 2))
Wet van 13 maart 2008 tot wijziging van de Wegenverkeerswet 1994 in verband met het aanmerken van het kentekenregister tot basisregistratie alsmede in verband met de herziening van de gegevensverstrekking uit het kentekenregister en enkele andere onderwerpen, Stb. 99 en het Kentekenreglement (het kentekenregister als basisregistratie voertuigen)
Hoofdstuk IVA van de Algemene wet inzake rijksbelastingen (basisregistratie inkomen)

Er wordt nog gewerkt aan diverse andere basisregistraties. Belangrijkste project is de Wet basisregistratie personen, waarin de Wet gemeentelijke basisadministratie persoonsgegevens zal opgaan. Een register kinderopvang is eveneens in voorbereiding.

## *4.9 Aanwijzingen voor de regelgeving*

De aanwijzingen 161 en 162 van de *Aanwijzingen voor de regelgeving* wijzen op de noodzaak om in een afzonderlijk deel van de toelichting bij een regeling waarin de beschikbaarheid van informatie van essentiële betekenis is aandacht te besteden aan de informatievoorziening. Dit voorschrift heeft een bredere strekking dan alleen aandacht te geven aan de bescherming van persoonsgegevens. Het ziet ook op de vraag welke informatie de overheid behoeft voor welke taak. In het bijzonder wordt nog verwezen naar het *Besluit informatievoorziening in de rijksdienst 1990* en de daarin neergelegde overlegverplichtingen over de informatieparagraaf in de toelichting.
Deze aanwijzingen zijn in het licht van de betekenis van de informatiemaatschappij voor de overheid, de plaats van de Wbp en het stelsel van basisregistraties overigens aan herziening toe.

# 5. Inhoud van de Wbp

Uiteraard zijn er gevolgen verbonden aan de toepassing van de Wbp. Wanneer er in een bijzondere wet wordt verwezen naar de Wbp is dat niet alleen een kwestie van een modelbepaling toepassen. Toepassing van de Wbp heeft materiële en procedurele gevolgen. In het onderstaande wordt een zeer beknopt overzicht gegeven van de belangrijkste categorieën van verplichtingen van verantwoordelijken en rechten van betrokkenen die voortvloeien uit de toepassing van de Wbp. Deze behandeling blijft beperkt tot hetgeen nodig is voor een goed begrip van de wetgevingsaspecten van de Wbp.

## 5.1 *Algemene normen voor de verwerking van persoonsgegevens*

*5.1.1 Plaats in de Wbp*
*Hoofdstuk 2, paragraaf 1, van de Wbp* bevat de algemene normen voor de verwerking van persoonsgegevens. Zij zijn van toepassing op alle verwerkingen en alle persoonsgegevens, uiteraard voor zover deze binnen de reikwijdte van de Wbp vallen.

*5.1.2 Algemene beginselen, proportionaliteit en subsidiariteit*
*Art. 6* Wbp verplicht tot verwerking van persoonsgegevens *in overeenstemming met de wet, en op behoorlijke en zorgvuldige wijze*. Hieruit vloeit in elk geval voort dat er geen buitenwettelijke verwerking van persoonsgegevens mag plaatsvinden. Met de verwijzing naar behoorlijkheids- en de zorgvuldigheidsnorm wordt beoogd om de gelding van de algemene zorgvuldigheidnorm uit het privaatrecht (artikel 6:162, tweede lid, BW) en de algemene beginselen van behoorlijk bestuur (afdeling 3.2 van de Awb en de ongeschreven beginselen) in het gegevensbeschermingsrecht te expliciteren. De wetgever heeft beoogd aan de Wbp ook de beginselen van *proportionaliteit en subsidiariteit* ten grondslag te leggen. Die beginselen vloeien rechtstreeks voort uit het noodzakelijkheidscriterium van artikel 8, tweede lid, van het EVRM, en de daarop gebaseerde jurisprudentie, en zijn daarom niet expliciet in de tekst van de Wbp terug te vinden. (Kamerstukken II 1997/98, 25 892, nr. 3, blz.9). Bij de vaststelling van onder meer de doeleinden van gegevensverwerking, rechtvaardigingsgronden voor verdere verwerking, bewaartermijnen en de verplichting tot dataminimalisatie moeten beslissingen van de verantwoordelijke voldoen aan deze beginselen.

*5.1.3 Doelbinding*

*Art. 7 Wbp* bevat het vereiste van de *doelbinding*. Gegevens worden alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld. Dit is in zekere zin de belangrijkste bepaling van het gegevensbeschermingsrecht. Let erop dat de Wbp het hier over *verzamelen* heeft. Het is het begin van het gegevensverwerkingsproces.
Doeleinden moeten *welbepaald* zijn, dus niet in te vage of te ruime termen zijn uitgedrukt. Doeleinden moeten *uitdrukkelijk omschreven* zijn. Dat kan op verschillende manieren plaatsvinden. Dat kan door middel van een melding aan het College bescherming persoonsgegevens of de functionaris voor de gegevensbescherming (art. 27 Wbp). Echter, ook de *wetgever* kan het doel van gegevensverzameling bepalen. In de meeste gevallen gaat de wetgever daartoe over wanneer gegevens ten behoeve van een publiekrechtelijke taak worden verzameld en daarvoor een specifieke regeling nodig is. Wanneer daartoe wordt overgegaan, wordt bij wet ook een verantwoordelijke aangewezen. Bevat de formele wet een doelomschrijving die voldoet aan de eisen van art. 7 Wbp dan bevordert dit de rechtszekerheid omdat hierdoor een nadere invulling aan het beoordelingskader is gegeven en het vereenvoudigt dit de meldingsformaliteiten. Gegevens mogen voorts alleen ten behoeve van *gerechtvaardigde* doeleinden worden verwerkt. Dat betekent dat het doeleinde uitsluitend op één van de wijzen, opgesomd in art. 8 Wbp moet kunnen worden bereikt. Zie de paragrafen 4.4.5 en 4.4.6 voor modelbepalingen en voorbeelden.

*5.1.4 Rechtvaardigingsgronden voor gegevensverwerking*

Art. 8 Wbp bevat een limitatieve opsomming van de gronden voor de *rechtvaardiging* van de verwerking van persoonsgegevens.
Persoonsgegevens worden slechts verwerkt indien:

a. de betrokkene daarvoor ondubbelzinnig *toestemming* heeft verleend
b. gegevensverwerking noodzakelijk is voor de uitvoering van een *overeenkomst* waarbij de betrokkene partij is (of het nemen van maatregelen in de precontractuele sfeer)
c. gegevensverwerking noodzakelijk is om een *wettelijke verplichting* na te komen waaraan de verantwoordelijke is onderworpen
d. gegevensverwerking noodzakelijk is ter vrijwaring van een *vitaal belang* van de betrokkene
e. gegevensverwerking noodzakelijk is voor de goede vervulling van een *publiekrechtelijke taak* door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt
f. gegevensverwerking noodzakelijk is voor de behartiging van het *gerechtvaardigde belang* van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Ter toelichting van deze rechtvaardigingsgronden kan het volgende worden opgemerkt:
*Toestemming* behoort altijd op ondubbelzinnige wijze voor een bepaalde gegevensverwerking, en op basis van behoorlijke informatie aan de betrokkene te worden gevraagd. De betrokkene moet in vrijheid zijn wil kunnen uiten.
Gegevensverwerking op grond van een *wettelijke verplichting* is alleen gerechtvaardigd wanneer het betreft verplichtingen die *bij of krachtens een in Nederland geldende wet* zijn gesteld, een verplichting tot het verwerken of doorgeven van gegevens krachtens enig wettelijk of ander voorschrift deel uitmakend van het recht van een *derde land* kan nooit op zichzelf een gegevensverwerking op grond van de Wbp rechtvaardigen; daarvoor is een *verdragsrechtelijke grondslag* nodig. Ontbreekt die, dan moet worden teruggevallen op een of meer van de andere gronden, genoemd in artikel 8.
Bij een *vitaal belang* moet met name worden gedacht aan een onmiddellijk en ernstig gevaar voor leven of gezondheid van de betrokkene.
De onder f genoemde grond vergt een *belangenafweging* door de verantwoordelijke.

*5.1.5 Verdere verwerking van persoonsgegevens - verstrekking voor een ander doel dan verzameling*
Art. 9 Wbp is een voor de wetgevingspraktijk bijzonder belangrijke bepaling. Het betreft de regeling van de *verdere verwerking* van persoonsgegevens. Verder verwerken betekent het verwerken van reeds verzamelde persoonsgegevens voor *andere* doelen dan waarvoor deze oorspronkelijk werden verzameld.
Art. 9, eerste lid, Wbp formuleert als beginsel dat persoonsgegevens niet verder worden verwerkt op een wijze die *onverenigbaar is met de doeleinden waarvoor zij zijn verkregen*. Dat betekent dat verdere verwerking als zodanig niet categorisch is uitgesloten, maar dat een nader oordeel gevormd moet worden over de (on)verenigbaarheid van een verdere verwerking. Uit art. 9, tweede lid, Wbp wordt duidelijk dat de verantwoordelijke met die oordeelsvorming is belast. De verantwoordelijke moet daarbij rekening houden met de verwantschap tussen oorspronkelijk en beoogd doel, met de aard van de gegevens, de gevolgen voor de betrokkene, de wijze waarop de gegevens zijn verkregen, en de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen. Het zal duidelijk zijn dat deze afweging alleen in concrete gevallen kan worden gemaakt.
In het belang van de opsporing van strafbare feiten en het belang van de veiligheid van de staat zijn enkele voorzieningen getroffen die impliciet of expliciet ontheffen van de afwegingsplicht. Zie de artikelen 126nc e.v., 126uc e.v. en 126zk van het Wetboek van Strafvordering en artikel 17 van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

*5.1.6 Verdere verwerking - status geheimhoudingsplichten*
Een extra aandachtspunt is dat art. 9, vierde lid, Wbp voorschrijft dat de verwerking achterwege blijft wanneer een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat. Wanneer de verstrekking van gegevens in de sfeer van *uitvoering, toezicht op de naleving en strafrechtelijke en bestuursrechtelijke handhaving van wettelijke regelingen* de verstrekking van persoonsgegevens tussen bestuursorganen en toezichthouders vergt, dan is een bijzondere wettelijke regeling in de regel noodzakelijk om: a. te verzekeren dat het doel van die verstrekking voldoende bepaald is omschreven,

en b. de vrijwel altijd geldende geheimhoudingsplicht rechtmatig te kunnen doorbreken. Daarvoor zijn een uitgebreid juridisch kader en modelbepalingen beschikbaar.

## 5.2 *Verstrekking van persoonsgegevens tussen bestuursorganen onderling*

De afgelopen jaren zijn er, speciaal in en voor de wetgevingspraktijk, oplossingen bedacht voor de wijze waarop gegevens, persoonsgegevens daaronder begrepen, tussen bestuursorganen onderling, tussen bestuursorganen en toezichthouders en tussen toezichthouders onderling kunnen worden verstrekt. De praktijk heeft uitgewezen dat daaraan grote behoefte bestaat. Onderlinge verstrekking verlaagt de toezichtslasten voor burgers en bedrijfsleven en vergroot tegelijk de effectiviteit van het toezicht. Veelal blijkt echter dat de geheimhoudingsplichten, bedoeld in paragraaf 5.1.6 daaraan in de weg kunnen staan. Die problematiek blijkt ook te bestaan op het bredere terrein van de onderlinge verstrekking van persoonsgegevens ten behoeve van de veiligheid. Zie daarvoor het eindrapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer "Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer" (bijlage bij de brief van de Ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties aan de voorzitter van de Tweede Kamer der Staten-Generaal van 10 februari 2009 (Kamerstukken II 2008/09, 28 684, nr. 199). De oplossingen zullen daarom mede in de vorm van wettelijke maatregelen moeten worden gegoten. Daartoe zijn onderstaande modelbepalingen ontworpen.
Het Ministerie van Justitie beziet nog of een algemene voorziening voor de oplossing van dit probleem in de Awb tot de mogelijkheden behoort. Zo dit mogelijk lijkt valt het overigens te verwachten dat met de verwezenlijking daarvan nog de nodige tijd is gemoeid.

Advies

Indien het noodzakelijk is om op structurele basis over te gaan op onderlinge verstrekking van persoonsgegevens tussen bestuursorganen of toezichthouders onderling of tussen bestuursorganen en toezichthouders, behoort aandacht te worden gegeven aan de vraag of de doeleinden voor die verstrekking voldoende zijn bepaald en of er geheimhoudingsplichten bestaan die hieraan in de weg staan.
Zonodig moet een afzonderlijke regeling op het niveau van de formele wet worden getroffen. Zie daarvoor de bijlage bij de brief van de Minister van Justitie van 29 oktober 2008 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2008/09, 31 700 VI, nr. 70), het rapport van de *Werkgroep herijking toezichtsregelgeving*, Den Haag, augustus 2008.
Gebruik bij het ontwerp van een wettelijke regeling onderstaande modelbepalingen.
Geef in de toelichting bij een dergelijke regeling in ieder geval een behoorlijk gemotiveerde rechtvaardiging van de beoogde gegevensverstrekking.

## Modelbepalingen gegevensverstrekking

### Variant I

1. *(Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken andere bestuursorganen de gegevens betreffende (doelomschrijving en betrokkenen aanduiden) welke zij behoeven voor de uitvoering van hun taak.*
2. *Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.*
3. *De in het eerste en tweede lid bedoelde gegevensverstrekking vindt niet plaats indien de persoonlijke levenssfeer van de betrokkene daardoor onevenredig wordt geschaad.*

of

### Variant II

1. *(Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken andere bestuursorganen de navolgende gegevens welke zij behoeven voor de uitvoering van hun taak:*

*a.(…)*
*b.(…)*
*c.(…) etc.*

2. *Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.*

of

### Variant III

1. *(Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken (naam bestuursorgaan of bestuursorganen) de navolgende gegevens ten behoeve van de goede uitvoering van (citeertitel of aanhaling regeling):*

*a.(…)*
*b.(…)*
*c.(…) etc.*

2. *Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.*

## Facultatieve bepalingen

*4 (of 3). Onverminderd artikel 10 van de Wet algemene bepalingen burgerservicenummer kunnen de bestuursorganen, bedoeld in het eerste en tweede lid, bij de verstrekking van gegevens op grond van het eerste of tweede lid gebruik maken van (omschrijving persoonsidentificerend nummer, anders dan het burgerservicenummer).*

*5 (of 4). Bij algemene maatregel van bestuur worden regels gesteld omtrent de gevallen waarin en de wijze waarop in ieder geval gegevens dienen te worden verstrekt.*

*6 (of 5). Bij de verstrekking van gegevens op grond van het eerste of tweede lid kunnen slechts bijzondere persoonsgegevens als bedoeld in artikel 16 van de Wet bescherming persoonsgegevens worden verstrekt, voor zover deze gegevens noodzakelijk zijn voor (doelomschrijving).*

*7(of 6). De gegevens, bedoeld in het voorgaande lid, worden verwerkt door (naam bestuursorgaan en/of toezichthouder dat/die als verantwoordelijke(n) word(t)(en) aangewezen). Zij kunnen slechts worden verwerkt door derden, voor zover deze betrokken zijn bij de uitvoering van deze wet en daartoe noodzakelijkerwijs de beschikking over deze gegevens verkrijgen.*

*8 (of 7). Bij algemene maatregel van bestuur/ regeling van Onze Minister worden regels gesteld ter waarborging van de persoonlijke levenssfeer. Daarbij wordt in elk geval geregeld:*

*a. op welke wijze de verwerking bedoeld in het zesde (of vijfde) lid, plaatsvindt;*

*b. op welke wijze door passende technische en organisatorische maatregelen deze gegevens worden beveiligd tegen verlies of onrechtmatige verwerking;*

*c. welke gegevens, aan welke personen of instanties, voor welk doel en op welke wijze kunnen worden verstrekt;*

*d. op welke wijze wordt gewaarborgd dat de verwerkte persoonsgegevens slechts worden verwerkt voor het doel waarvoor zij zijn verzameld of voor zover het verwerken met dat doel verenigbaar is, alsmede hoe daarop wordt toegezien.*

*9 (of 8). (Naam bestuursorgaan) benoemt een functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de Wet bescherming persoonsgegevens/ een privacyfunctionaris die toeziet op de verwerking van persoonsgegevens krachtens het eerste/ krachtens het eerste en tweede lid.*

## Toelichting

### Algemeen

Toezichthouders, respectievelijk de bestuursorganen waaraan zij verantwoording schuldig zijn, dienen hun toezichtactiviteiten doelmatig in te richten. Een doelmatig toezicht betekent in ieder geval ook dat de maatschappelijke toezichtslast zoveel mogelijk wordt beperkt. Verschillende toezichthouders, belast met het toezicht op de naleving van verschillende wetten die betrekking hebben op één keten of één domein brengen hun activiteiten daartoe zoveel mogelijk samen en oefenen hun bevoegdheden zoveel mogelijk op een onderling afgestemde wijze uit. Een effectief keten- of domeintoezicht

betekent dat de betrokken samenwerkende toezichthouders of bestuursorganen over en weer moeten kunnen beschikken over elkaars relevante gegevens.
Zodra deze gegevens moeten worden aangemerkt als persoonsgegevens in de zin van artikel 1, onder a, van de Wet bescherming persoonsgegevens verdient het aandacht dat persoonsgegevens door elke afzonderlijke toezichthouder uitsluitend mogen worden verzameld ten behoeve van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. De overdracht van persoonsgegevens aan een andere toezichthouder die deze vervolgens verwerkt ten behoeve van een ander doel is hiermee niet zonder meer verenigbaar. Artikel 9 van de Wet bescherming persoonsgegevens maakt het weliswaar mogelijk om persoonsgegevens verder te verwerken ten behoeve van andere doeleinden dan waarvoor zij zijn verzameld, maar de afweging die de verantwoordelijke op grond van die bepaling moet maken is in de praktijk niet steeds eenvoudig te maken. Bovendien staan geheimhoudingsbepalingen niet zelden uiteindelijk in de weg aan overdracht van persoonsgegevens. De correcte toepassing van de aan artikel 9 van de Wet bescherming persoonsgegevens ten grondslag liggende regels (met name zij gewezen op artikel 6, eerste lid, onder b, van richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281)) en beginselen kan bij wet echter nader worden vormgegeven. Bij (of krachtens) de wet kan zo nauwkeurig mogelijk worden aangegeven welke toezichthouders of bestuursorganen ten behoeve van welke doelen en onder welke omstandigheden welke persoonsgegevens mogen overdragen of ontvangen naar, respectievelijk van, andere bestuursorganen. Daartoe kunnen één of meer van de hierboven weergegeven modellen worden benut.
Vaststelling van een dergelijke regeling in elk van de daarvoor in aanmerking komende wetten komt alleen in beeld wanneer de desbetreffende keten of het desbetreffende domein een duidelijke bestendigheid kent. Zie in dit verband ook aanwijzingen 6 en 10 van de Aanwijzingen voor de regelgeving. Een dergelijke regeling heft overigens niet de bestaande verantwoordelijkheden (artikel 1, onder d, Wbp) of de meldplicht (artikel 27 Wbp) en de transparantieverplichtingen (artikelen 33 en 34 Wbp) ten aanzien van overdracht op. Evenmin doet een dergelijke regeling afbreuk aan de rechten van inzage, correctie en verzet van de betrokkene (artikelen 35, 36 en 40 Wbp) en de beveiligingsplicht (artikel 13 Wbp).

### Modelbepalingen eerste en tweede lid

Het centrale element van een overdrachtsregeling bestaat uit de verplichting voor de desbetreffende bestuursorganen en toezichthouders elkaar wederzijds gegevens uit te wisselen. In alle gevallen moet er, gelet op artikel 7 van de Wet bescherming persoonsgegevens, een uitdrukkelijke omschrijving van het doel van de overdracht aan worden toegevoegd. In veel gevallen kan, waar het gaat om het bestuursorgaan waaraan gegevens moeten worden overgedragen worden volstaan met een verwijzing naar de uitvoering van de taak van het desbetreffende bestuursorgaan. Daarbij wordt voorondersteld dat die taak

in andere wetgeving behoorlijk is omschreven. Dit dient uiteraard wel te worden nagegaan. Voorzover blijkt dat dit elders niet of niet behoorlijk is vastgelegd, dient dit doel alsnog te worden geëxpliciteerd. Zie hiervoor het eerste lid van de drie hierboven weergegeven varianten. Voor een voorbeeld zij verwezen naar artikel 107, eerste lid, van de Vreemdelingenwet 2000.
Voor zover het betreft de doelomschrijving voor het ontvangen van elders verwerkte gegevens, dient de doelomschrijving beperkt te blijven tot de uitvoering en het toezicht op de naleving van de wet waarin de overdrachtsregeling wordt opgenomen. Dit is in het tweede lid van de drie varianten uitgewerkt.

Varianten

Uit het oogpunt van bescherming van persoonsgegevens verdient het de voorkeur om de overdrachtsregeling zo nauwkeurig mogelijk te beperken tot de gegevens waarvan de noodzaak tot overdracht vaststaat. De praktijk leert dat het niet in alle gevallen goed mogelijk is hier een volledig beeld van te krijgen. Om die reden worden hier drie varianten voorgesteld.
Variant I komt in aanmerking wanneer het niet mogelijk blijkt om een nauwkeurige opsomming te geven van de gegevens die moeten worden overgedragen en wanneer moet worden teruggegrepen op min of meer algemene omschrijvingen van het doel van de overdracht, de gegevens die het betreft en de kring van betrokkenen op wie de gegevens betrekking hebben. In combinatie met het feit dat het eerste en tweede lid geen onderscheid maken tussen gegevens in algemene zin en persoonsgegevens in het bijzonder, dient in deze variant een toetsingsplicht van het verantwoordelijk bestuursorgaan te worden opgenomen. Wanneer het gaat om de verstrekking van persoonsgegevens dient het bestuursorgaan een afweging te maken waarbij het belang van het toezicht en het belang van de bescherming van persoonsgegevens tegen elkaar worden afgewogen. Aspecten van subsidiariteit en proportionaliteit behoren daarbij tot uitdrukking te komen.
Variant II komt in aanmerking waarbij een limitatieve opsomming van de over te dragen gegevens mogelijk blijkt. Desgewenst kan ook het tweede lid van deze variant overeenkomstig het eerste lid worden uitgewerkt.
Variant III komt in aanmerking wanneer het mogelijk is de concrete aanduiding van de gegevens te combineren met een aanduiding van de concrete wettelijke regeling die door het bestuursorgaan waaraan de verstrekking plaatsvindt wordt uitgevoerd. Aangezien in de varianten II en III sprake is van een exacte opsomming van de gegevens bij wet, is het zeker wanneer er waarborgen zijn opgenomen in de vorm van de facultatieve bepalingen, de rechten van betrokkenen behoorlijk zijn gewaarborgd en het interne toezicht is geregeld, niet noodzakelijk aan de desbetreffende bestuursorganen of toezichthouders nog een expliciete verplichting tot afweging tussen de belangen die worden gediend met gegevensverstrekking en het belang van de bescherming van persoonsgegevens op te leggen.

## Facultatieve bepalingen

In sommige gevallen is het noodzakelijk of wenselijk de over te dragen gegevens te combineren met een persoonsidentificerend nummer. In verband met artikel 24 Wet bescherming persoonsgegevens is daarvoor steeds een uitdrukkelijke wettelijke grondslag vereist. In verreweg de meeste gevallen zal volstaan kunnen worden met het burgerservicenummer. De algemene grondslag voor het gebruik van dit nummer is neergelegd in artikel 10 van de Wet algemene bepalingen burgerservicenummer. Een afzonderlijke wettelijke regeling voor het gebruik van het burgerservicenummer is dan ook niet nodig. Voor het gebruik van het sofinummer is ook reeds een wettelijke grondslag beschikbaar (de Algemene wet inzake rijksbelastingen). Wel moet bij nieuwe gebruiksmogelijkheden het Besluit sofi-nummer Wbp worden aangepast. Daarvoor is overleg met de directie Wetgeving van het Ministerie van Justitie vereist.
In sommige sectoren worden echter andere persoonsidentificerende nummers gebruikt. Daarvoor is wel een afzonderlijke wettelijke grondslag benodigd. Het vierde lid voorziet daarin.
Indien de behoefte bestaat tot nadere regeling van de gevallen waarin gegevens mogen of moeten worden verstrekt en het noodzakelijk is onderscheid aan te brengen in die gevallen, kan het doelmatig zijn dit in lagere regelgeving uit te werken. Zo kan bijvoorbeeld worden gedacht aan de keuze of de gegevens in individuele gevallen moeten worden verstrekt, of dat juist online toegang tot een databank waarin deze gegevens zich bevinden is toegestaan. Het vijfde lid voorziet in een delegatiegrondslag voor een algemene maatregel van bestuur waarin een dergelijke uitwerking kan plaatsvinden.
De verwerking van bijzondere persoonsgegevens in de zin van artikel 16 Wet bescherming persoonsgegevens is verboden, tenzij de Wet bescherming persoonsgegevens daartoe een specifieke grondslag biedt. Dat geldt ook voor zover de verwerking bestaat uit de overdracht van die gegevens. Uit het systeem van de desbetreffende paragraaf van de Wet bescherming persoonsgegevens vloeit voort dat daarvoor in veel gevallen in een bijzondere wet een specifieke regeling wordt getroffen. Daarbij dient de doelomschrijving nauwkeurig te worden geformuleerd. Ook dient de verantwoordelijke expliciet te worden aangeduid. De aard van de gegevens brengt verder mee dat een restrictieve benadering van het gebruik daarvan uitgangspunt is. Zo verdient het aanbeveling tenminste in een gedelegeerde regeling voorschriften met betrekking tot organisatorische en technische beveiliging en een specifieke verstrekkingsregeling op te nemen. Ook dient aandacht te worden gegeven aan de omstandigheid dat de gegevens bij verwerking door een ontvanger van deze gegevens mede worden verwerkt door derden die niet de status hebben van een bewerker in de zin van de Wet bescherming persoonsgegevens. Het zesde, zevende en achtste lid bevatten daarvoor een voorziening.
Tenslotte kan het zinvol zijn om een aanvullende waarborg in de vorm van benoeming van een functionaris voor de gegevensbescherming in de zin van artikel 62 van de Wbp, of een privacyfunctionaris, al dan niet in de zin van artikel 35 Wet politiegegevens, te benoemen. Gegevensverstrekking is doorgaans een complexe zaak voor de betrokken bestuursorganen en ambtenaren. Goed toezicht voorkomt het maken van fouten,

verhoogt de kwaliteit van de gegevens en kan bijdragen aan het vergroten van het vertrouwen van het publiek in de gegevensverstrekking. De wetgeving kent diverse voorbeelden van privacytoezichthouders, die over enige bevoegdheden en verplichtingen beschikken.

## 5.3 Andere algemene normen voor de verwerking van persoonsgegevens

Art. 10 Wbp geeft een algemeen geformuleerde gedragslijn voor de hantering van *bewaartermijnen*. De Wbp geeft zelf geen concrete termijnen. Doeleinden van verzameling en (verdere) verwerking zijn bepalend voor de vaststelling van de bewaartermijn.
Art. 11 Wbp geeft een algemeen geformuleerde regeling voor de *dataminimalisatie*: alleen die gegevens mogen worden verwerkt die toereikend, ter zake dienend en niet bovenmatig zijn. De verantwoordelijke dient in te staan voor de *kwaliteit* van deze data.
Art. 12 Wbp geeft een *geheimhoudingsregeling* voor personen die handelen onder het gezag van een verantwoordelijke en voor bewerkers.
Art. 13 Wbp regelt de *beveiligingplicht*. De verantwoordelijke moet passende *technische en organisatorische maatregelen* treffen om verlies of onrechtmatige verwerking van gegevens zoveel mogelijk te voorkomen. Zie in dit verband ook artikel 41 van de Kaderwet zelfstandige bestuursorganen.
De artt. 14 en 15 Wbp regelen de rechtsverhouding tussen verantwoordelijke en *bewerker*.

## 5.4 Verwerking van bijzondere persoonsgegevens

*5.4.1 Verwerkingsverbod en uitzonderingen daarop*
*Bijzondere persoonsgegevens* zijn persoonsgegevens met betrekking tot: godsdienst of levensovertuiging, ras (of etniciteit), politieke gezindheid, gezondheid, seksueel levensgedrag, of het lidmaatschap van een vakvereniging. Met bijzondere persoonsgegevens worden gelijkgesteld strafrechtelijke persoonsgegevens of gegevens betreffende onrechtmatig of hinderlijk gedrag naar aanleiding van een opgelegd verbod naar aanleiding van dat gedrag.
Ingevolge art. 16 Wbp is het verwerken van bijzondere persoonsgegevens *verboden*, behoudens een uitdrukkelijke regeling in de Wbp, of een van de Wbp afwijkende wet. Om systematische redenen wordt deze materie behandeld in de paragrafen 4.7.2 tot en met 4.7.6 van deze leidraad.

*5.4.2 Persoonsidentificerende nummers*
Persoonsidentificerende nummers zijn als zodanig door de Europese en Nederlandse wetgever niet aangemerkt als bijzondere persoonsgegevens. Niettemin worden deze nummers wel op gelijke wijze als bijzondere persoonsgegevens benaderd, waar het gaat om de wijze waarop de wetgever daarmee moet omgaan. Zie daarvoor paragraaf 4.7.6.

## 5.5 Bestuursrechtelijke instrumenten in de Wbp

In dit onderdeel wordt enige toelichting gegeven op twee bijzondere bestuursrechtelijke instrumenten die de Wbp kent, de *meldplicht en het voorafgaand onderzoek*. Beide instrumenten hebben een zekere preventieve werking. De behandeling blijft beperkt tot datgene wat voor de wetgevingspraktijk van belang is.

*5.5.1 Meldplicht*

Ingevolge artt. 27 en 28 Wbp moet een verwerking van persoonsgegevens, voordat de verwerking aanvangt, worden *gemeld* bij het College bescherming persoonsgegevens of, indien deze aanwezig is, bij de functionaris voor de gegevensbescherming. De meeste ministeries beschikken over een functionaris. Het doel van de meldplicht is de verantwoordelijke ertoe te brengen zoveel mogelijk transparantie te verschaffen over de door hem verrichte verwerkingen van persoonsgegevens. Voor zover de wetgever dat niet reeds heeft bepaald, moet de melding de identiteit van de verantwoordelijke, de doeleinden van de gegevensverwerking, de aard van de te verwerken gegevens, de ontvangers van gegevens, de voorgenomen doorgiften naar landen buiten de Europese Unie, en een algemene beschrijving van de maatregelen ter beveiliging van persoonsgegevens die tot doel heeft om te kunnen beoordelen of de beveiligingsplicht en de verplichtingen van een bewerker kunnen worden nageleefd (art. 28 Wbp). De melding behelst ook de doeleinden waarvoor de gegevens oorspronkelijk worden verzameld.
Het niet naleven van de meldplicht is zowel met een *strafrechtelijke* als met een *bestuursrechtelijke boete* bedreigd (artt. 66 en 75 Wbp). Ook het opleggen van een *last onder bestuursdwang of een last onder dwangsom* is mogelijk (art. 65 Wbp).
Op grond van art. 29 Wbp kan voor veel voorkomende verwerkingen bij algemene maatregel van bestuur *vrijstelling* van de meldplicht worden verleend. Criterium hiervoor is dat het moet gaan om verwerkingen waarbij de inbreuk op fundamentele rechten en vrijheden van de betrokkene onwaarschijnlijk is.

*5.5.2 Vrijstellingsbesluit Wbp*

In het *Vrijstellingsbesluit Wbp* zijn een groot aantal veel voorkomende verwerkingen in tal van maatschappelijke sectoren onder voorwaarden vrijgesteld van de meldplicht. Het Vrijstellingsbesluit Wbp valt onder de verantwoordelijkheid van de Minister van Justitie. In het kader van de noodzaak tot administratieve lastenverlichting voert de Minister van Justitie een in beginsel ruimhartig vrijstellingsbeleid.

Advies

Voorstellen tot aanpassing van het Vrijstellingsbesluit Wbp kunnen, mits voldoende gemotiveerd tot het Ministerie van Justitie, directie Wetgeving worden gericht. Het Ministerie van Justitie zal deze voorstellen overigens bespreken met het georganiseerd bedrijfsleven en het College bescherming persoonsgegevens.

*5.5.3 Overige vrijstellingen - opsporing van strafbare feiten, openbare registers*
Vrijstelling van de meldplicht is, op grond van art. 29, derde lid, Wbp, ook mogelijk voor bij algemene maatregel van bestuur aan te wijzen verwerkingen die worden verricht door verantwoordelijken die krachtens de wet met de *opsporing van strafbare feiten* zijn belast. Sinds de totstandkoming van de *Wet politiegegevens* en de *Wet op de bijzondere opsporingsdiensten* is de ruimte voor dergelijke regelgeving gering.
*Bij de wet* ingestelde *openbare registers*, of verstrekkingen van persoonsgegevens door bestuursorganen krachtens een *wettelijke verplichting* zijn eveneens vrijgesteld van de meldplicht.

Voorbeelden van openbare registers

Artikel 8 Kadasterwet
Artikel 21 Handelsregisterwet 2007
Artikelen 19 en 19a Faillissementswet
Artikel 30 Wet bescherming persoonsgegevens

*5.5.4 Voorafgaand onderzoek*
Een melding bij het College bescherming persoonsgegevens of de functionaris voor de gegevensbescherming is een administratieve verplichting. Alleen het nalaten aan deze verplichting te voldoen heeft rechtsgevolg, dan treedt strafbaarheid in. Met nadruk wordt erop gewezen dat het voldoen aan deze verplichting wel een noodzakelijke, maar niet altijd een voldoende voorwaarde is om een verwerking als zijnde in alle opzichten rechtmatig te kunnen aanmerken. Het naleven van de meldplicht is geen impliciet rechtmatigheidsoordeel van het Cbp.
Dat ligt anders bij een *voorafgaand onderzoek*. Een voorafgaand onderzoek eindigt in een verklaring van het Cbp omtrent de rechtmatigheid van de verwerking (art. 32 Wbp). De wetgever heeft ervoor gekozen om dit instrument slechts voor een beperkt aantal typen verwerkingen voor te schrijven (art. 31 Wbp). Het betreft voornamelijk het gebruik van persoonsidentificerende nummers ten behoeve van andere doeleinden dan waarvoor dit nummer noodzakelijk is, voor het verzamelen van gegevens zonder dat de betrokkene daarvan op de hoogte is, of het gebruik van strafrechtelijke persoonsgegevens door particulieren.
Uit wetgevingsperspectief is belangrijk dat *openbare registers die bij de wet zijn ingesteld niet* kunnen worden onderworpen aan een voorafgaand onderzoek. *Bij wet of bij algemene maatregel van bestuur* kunnen verwerkingen worden aangewezen die aan een voorafgaand onderzoek kunnen worden onderworpen (art. 32, derde lid, Wbp). Het Cbp kan in zijn jaarverslag de wenselijkheid daartoe aangeven.
Met deze mogelijkheid moet terughoudend worden omgegaan. Voorafgaande onderzoeken nemen, mede als gevolg van de toepasselijkheid van afdeling 3.4 van de Awb, veel tijd in beslag en leiden tot administratieve lasten en nalevingskosten.

Advies

Besteed bij de voorbereiding van wetgeving met betrekking tot de bescherming van persoonsgegevens aandacht aan het effect dat de toepassing van preventieve instrumenten uit de Wbp als de meldplicht en het voorafgaand onderzoek heeft op administratieve lasten en nalevingskosten. Benut waar mogelijk alternatieve mogelijkheden als vrijstelling van de meldplicht of instelling van intern toezicht in plaats van het aanvragen van een voorafgaand onderzoek.
Voor zover de noodzaak mocht bestaan om bij wet of amvb verwerkingen aan te wijzen die aan een voorafgaand onderzoek moeten worden onderworpen wordt afstemming met het Ministerie van Justitie, Directie Wetgeving gezocht. Op een voorstel van wet of een ontwerpbesluit moet een advies van het College bescherming persoonsgegevens worden gevraagd.

## *5.6 Transparantie en rechten betrokkene en de uitzonderingen daarop*

De hoofdstukken 5 en 6 van de Wbp bevatten belangrijke bepalingen ten behoeve van de bescherming van de persoonsgegevens van betrokkenen. Het betreft de transparantievoorschriften en de rechten van de betrokkene. Het is niet goed mogelijk in het bestek van deze leidraad in te gaan op de gedetailleerde regeling van deze rechten. In het onderstaande worden alleen punten opgenomen die van bijzondere betekenis zijn voor de wetgevingspraktijk.

### *5.6.1 Transparantievoorschriften*

Hoofdstuk 5 Wbp bevat *transparantievoorschriften*. Op grond van artikel 33 Wbp dient de verantwoordelijke de betrokkene op de hoogte te stellen van zijn identiteit en de doeleinden van gegevensverwerking, alsmede andere informatie die nodig is om de betrokkene een behoorlijke en zorgvuldige verwerking van de hem betreffende gegevens te waarborgen. Artikel 34 Wbp betreft een bijzondere regeling voor de transparantieverplichting voor de gevallen waarin de gegevens niet rechtstreeks van de betrokkene zijn verkregen maar langs andere weg, bijvoorbeeld via derden, zijn verzameld.
Deze leidraad is niet de plaats om uitgebreid in te gaan op functie en betekenis van de transparantievoorschriften. Wel moet worden benadrukt dat deze voorschriften tot doel hebben burgers in een positie te brengen van waaruit zij in staat zijn actief hun rechten op inzage, correctie en verzet uit te oefenen.
Daarom behoort bij het ontwerpen van wettelijke voorschriften waarin de verwerking van persoonsgegevens een belangrijke plaats inneemt aandacht te worden geschonken aan de manier waarop verantwoordelijken - zeker wanneer dit bestuursorganen zijn - in concreto uitvoering geven aan de artt. 33 en 34 Wbp. Gelet op de aard van deze verplichting zijn aanvullende wettelijke regels hier niet het eerst in aanmerking komende middel. Andere mogelijkheden, met name in de sfeer van publieksvoorlichting, lijken eerder in aanmerking te komen. Besteed daaraan aandacht in de toelichting.

Overigens dragen ook de meldplicht en de meldingenregisters van Cbp en de functionaris van de gegevensbescherming bij aan de transparantie.

Advies

Besteed in voorkomende gevallen in een memorie van toelichting of nota van toelichting aandacht aan de wijze waarop een bestuursorgaan, dat in de desbetreffende wet of algemene maatregel van bestuur als verantwoordelijke voor de verwerking van persoonsgegevens wordt aangewezen, inhoud geeft aan zijn verplichtingen voortvloeiend uit hoofdstuk 5 Wbp.

*5.6.2 Rechten betrokkene*
De betrokkene heeft op grond van hoofdstuk 6 Wbp diverse rechten toegekend gekregen. De rechten op kennisname en verbetering vormen een uitwerking van artikel 10, derde lid, van de Grondwet. Mede door dit grondrechtelijk karakter wordt in bijzondere wetten in beginsel niet afgeweken van de regeling van de Wbp.

*5.6.2.1 Recht van inzage*
Het *recht van inzage* (art. 35 Wbp). De betrokkene heeft het recht om te weten welke persoonsgegevens door de verantwoordelijke worden verwerkt, voor welke doeleinden en aan welke derden deze gegevens zijn verstrekt.

*5.6.2.2 Recht van correctie*
Het *recht van correctie* (art. 36 tem 38 Wbp). De betrokkene heeft het recht de verantwoordelijke te verzoeken hem betreffende gegevens te verbeteren, aan te vullen, af te schermen, of te verwijderen bij feitelijke onjuistheden, bij verwerking ten behoeve van onvolledige of niet terzake dienende doelen of bij verwerkingen die in strijd met een wettelijk voorschrift worden verricht.

*5.6.2.3 Recht van verzet*
Het *recht van verzet* (artt. 40 en 41 Wbp). De betrokkene heeft, in bepaalde gevallen en onder bepaalde voorwaarden, het recht verzet aan te tekenen tegen de verwerking van zijn persoonsgegevens.

*5.6.2.4 Recht om niet onderworpen te worden aan besluiten met rechtsgevolgen door volledig geautomatiseerde verwerkingen*
*Het recht om niet te worden onderworpen aan besluiten met rechtsgevolgen, voortvloeiend uit volledig geautomatiseerde verwerkingen* die zijn bestemd om een beeld te krijgen van zijn persoonlijkheid (art. 42 Wbp). De betrokkene heeft bij verwerkingen met dergelijke vérstrekkende consequenties een recht op menselijke tussenkomst, voorafgaande aan het nemen van het besluit.

*5.6.3 Uitzonderingsbepalingen*

De rechten van betrokkene zijn niet absoluut van aard. De rechten van correctie en verzet kennen een aantal *bijzondere uitzonderingsgronden*. Ook houdt de wet rekening met de positie van derden. Verder geldt het recht van verzet niet ten aanzien van de verwerking van *persoonsgegevens in openbare registers die bij de wet zijn ingesteld (art. 40, vierde lid, Wbp).*

*5.6.4 Artikel 43 Wbp*

Een voor de praktijk belangrijke bepaling is art. 43 Wbp. Deze bepaling formuleert een *algemene uitzondering* op bepaalde (niet alle) rechten van de betrokkene. Die uitzondering geldt ten aanzien van:

- de plicht tot afweging die de verantwoordelijke moet maken alvorens gegevens met toepassing van art. 9, eerste lid, Wbp door te geven aan een derde
- de inlichtingenverstrekking over de van de meldplicht vrijgestelde verwerkingen
- de transparantieverplichtingen
- het recht op inzage

De verantwoordelijke mag die verplichtingen buiten toepassing laten voor zover dat noodzakelijk is in het belang van:

- de veiligheid van de staat
- de voorkoming, opsporing en vervolging van strafbare feiten
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen
- het toezicht op de naleving van wettelijke voorschriften, gesteld ten behoeve van bovengenoemde opsporings- en financiële belangen
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen

De aard van art. 43 Wbp brengt met zich dat deze bepaling alleen van geval tot geval kan worden ingeroepen. Hoewel dit artikel potentieel een belangrijke rol kan spelen in de bescherming van de belangen van de overheid, in aanvulling op de bepalingen waarin reeds expliciet de belangen van de overheid zijn verdisconteerd, beperkt de toepassing van art. 43 Wbp zich tot bijzondere gevallen en sluit de aard van deze bepaling nagenoeg uit dat op grond daarvan *beleidsregels* worden vastgesteld.

Er bestaan overigens diverse bepalingen in bijzondere wetten die *andere belangenafwegingen voorschrijven*, zoals artikel 67, tweede lid, van de Algemene wet inzake rijksbelastingen en afdeling 1.5.1 van de Wet op het financieel toezicht.

Advies

Artikel 43 Wbp wordt niet gebruikt als grondslag voor systematische gegevensverstrekking tussen verantwoordelijken. Voor systematische gegevensverstrekking is veelal een afzonderlijke wettelijke regeling noodzakelijk. Artikel 43 Wbp is daarom geen voldoende duidelijke grondslag voor de vaststelling van beleidsregels.

## 5.7 Overige bepalingen van de Wbp

Aan de positie en de rol van het College bescherming persoonsgegevens wordt in paragrafen 6.1, 6.2, 6.3 en 8.2 van deze leidraad aandacht gegeven. Toezicht op de naleving en handhaving van de Wbp worden in paragraaf 6 behandeld.

## 5.8 Gegevensverkeer met landen buiten de EU/EER

Bij het ontwerpen van wettelijke voorschriften over de verwerking van persoonsgegevens behoort aandacht te worden gegeven aan de vraag of de desbetreffende gegevensverwerking (mede) bestemd is om naar het buitenland te worden doorgegeven. Het voert binnen het bestek van deze leidraad te ver om de gecompliceerde regeling van de artt. 25 en 26 van richtlijn nr. 95/46/EG en hoofdstuk 11 van de Wbp geheel uiteen te zetten. Die voorschriften bevatten het recht dat van toepassing is op het gegevensverkeer naar landen buiten de EU. Niettemin volgen hier enige hoofdtrekken.
De richtlijn beoogt de EU aan te merken als *één ruimte waarbinnen persoonsgegevens - mits die in overeenstemming met richtlijn worden verwerkt - vrijelijk kunnen circuleren*. Het beschermingsniveau van de richtlijn wordt verondersteld van hoog niveau te zijn. Niettemin laat de richtlijn de lidstaten een behoorlijke mate van vrijheid in de implementatie van de richtlijn. Dat betekent dat er verschillen bestaan in de implementatiewetgeving tussen de lidstaten onderling.
Het niveau van gegevensbescherming dat de richtlijn garandeert, geldt niet slechts in de EU, maar ook in de *EER.* Sinds *Besluit van het Gemengd Comité van de EER nr. 83/1999 van 25 juni 1999 tot wijziging van Protocol nr. 37 en bijlage XI (Telecommunicatiediensten) bij de EER-Overeenkomst (PbEG 2000 L 296)* geldt het regime voor derde landen - een uitzondering daargelaten - uitsluitend voor de landen die geen deel uitmaken van de EER.
Voor de niet van de EU en de EER deel uitmakende landen geldt het *regime voor gegevensoverdracht naar derde landen*. Gegevensexport naar die landen is in beginsel slechts toegestaan als is vastgesteld dat in dat land een *passend niveau van gegevensbescherming* heerst. De beoordeling daarvan is primair een taak van de verantwoordelijke. Niettemin heeft de Europese Commissie een klein aantal landen aangewezen waar naar haar oordeel een passend niveau van gegevens bestaat. Naar die landen kunnen persoonsgegevens zonder aanvullende garanties worden overgedragen. Een indicatie of een land overigens als zodanig kan worden aangemerkt is of het desbetreffende land tot het Dataprotectieverdrag is toegetreden. Toetreding tot dat verdrag is ook mogelijk voor landen die geen lid zijn van de Raad van Europa.
Bedenk dat ook de overdracht van gegevens tussen verantwoordelijken in Nederland en de *BES-eilanden* onder het regime voor grensoverschrijdend gegevensverkeer valt. De BES-eilanden zijn immers noch deel van de EU, noch van de EER. Hetzelfde geldt voor het gegevensverkeer tussen Nederland en de Caribische delen van het Koninkrijk, Curaçao, Aruba en Sint Maarten.

Advies

Raadpleeg voor nadere informatie over gegevensverkeer met landen buiten de EU en de EER de brief van de Minister van Justitie van 9 maart 2000 aan de voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 1999/2000, 27 043, nr.1). Op de website van het Cbp is ook de nodige achtergrondinformatie te vinden over dit onderwerp.

# 6. Toezicht op de naleving en bestuursrechtelijke en strafrechtelijke handhaving

## *6.1 Toezicht op de naleving en handhaving van de Wbp en andere wetgeving op het gebied van de bescherming van persoonsgegevens*

De Wbp en - in beginsel - alle overige gegevensbeschermingsregelgeving wordt bestuursrechtelijk gehandhaafd. Daartoe is aan het Cbp het toezicht op de naleving op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde toevertrouwd (artikelen 51 en 61 Wbp). Nu de bepalingen van de Wbp en de overige relevante wetgeving in een in beginsel onbeperkt aantal sectoren van het maatschappelijk leven toepassing vinden, betekent dit dat ook de taakomschrijving van het Cbp - voor zover het betreft het nalevingstoezicht op de Wbp - niet gerelateerd is aan specifieke sectoren van bedrijvigheid. In dat opzicht laat het Cbp zich vergelijken met bijvoorbeeld de Nederlandse mededingingsautoriteit, maar bijvoorbeeld niet met de Onafhankelijke Post- en Telecommunicatieautoriteit, De Nederlandsche Bank, de Autoriteit Financiële Markten of de Inspectie voor de Gezondheidszorg. Laatstgenoemde organen zijn belast met het toezicht op min of meer afgebakende sectoren van bedrijvigheid.
Dat heeft consequenties voor de wetgevingspraktijk. Het algemene karakter van de Wbp brengt met zich dat in voorstellen van wet, ook wanneer die sectorspecifieke regelingen bevatten met betrekking tot persoonsgegevens, in beginsel geen sectorspecifieke toezichthouders in het leven worden geroepen die (mede) zijn belast met het toezicht op de naleving van bepalingen met betrekking tot bescherming van persoonsgegevens.
In beginsel, want op die regel zijn enkele uitzonderingen aanvaard.
In de eerste plaats kan uit een *bindend EU-besluit* voortvloeien dat het toezicht op de naleving op bepalingen met betrekking tot gegevensbescherming geheel of gedeeltelijk of mede moet wordt opgedragen aan een ander orgaan dan de toezichthoudende autoriteit in de zin van richtlijn nr. 95/46/EG. Uitwerkingen daarvan zijn te vinden in de Wet op het financieel toezicht.
In de tweede plaats kan het in verband met de *noodzakelijke samenhang tussen onderdelen van een wetgevingscomplex* dat een gehele sector omvat noodzakelijk zijn dat een sectorspecifieke toezichthouder mede nalevingstoezicht uitoefent op sectorspecifieke regelingen met betrekking tot de bescherming van persoonsgegevens. Daarvoor behoort overigens een grondige motivering te worden gegeven. Een voorbeeld is de Telecommunicatiewet. De desbetreffende regels (hoofdstuk 11 van die wet) worden zowel door de OPTA, als door het Cbp gehandhaafd. In een dergelijk geval moet nadrukkelijk worden overwogen in de desbetreffende wet een verplichting tot het sluiten van een samenwerkingsprotocol op te nemen om een onnodige toezichtslast voor de sector te voorkomen en om zonodig toezichtgegevens te kunnen uitwisselen.
Indien wordt overwogen op een van deze uitzonderingen een beroep te doen, vindt

voorafgaand overleg met de directie Wetgeving van het Ministerie van Justitie plaats.
In de derde plaats kan voor *terreinen die niet door richtlijn nr. 95/46/EG, richtlijn nr. 2002/58/EG of kaderbesluit nr. 2008/977/JBZ worden bestreken* een ruimere mogelijkheid worden aangenomen om het toezicht op specifieke gegevensbeschermingsbepalingen aan een ander orgaan op te dragen. Te denken valt aan de Wet op de inlichtingen- en veiligheidsdiensten 2002. In die wet is de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten aangewezen als toezichthouder.
Volledigheidshalve wordt vermeld dat het Cbp ook het toezicht op de naleving uitoefent van de *Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens,* de *Wet gemeentelijke basisadministratie persoonsgegevens* en deelneemt aan het - soms collectief georganiseerde - nalevingstoezicht op diverse Europeesrechtelijke regelingen.

Advies
Het toekennen van toezicht op de naleving van wettelijke bepalingen met betrekking tot de bescherming van persoonsgegevens en die vallen onder de reikwijdte van richtlijn nr. 95/46/EG, van richtlijn nr. 2002/58/EG of van kaderbesluit nr. 2008/977/JBZ, aan andere organen dan het Cbp is alleen in zeer bijzondere gevallen mogelijk. In alle gevallen waarin dit wordt overwogen vindt voorafgaand overleg met de directie Wetgeving van het Ministerie van Justitie plaats.

Ook overigens verdient het onderwerp extern of intern toezicht op de naleving van de wetgeving nadrukkelijk aandacht. De praktijk leert dat ook dat de Tweede en Eerste Kamer daaraan veel belang toekennen. (Zie de uitkomst van een door de Eerste Kamer georganiseerde expertbijeenkomst over gegevensbescherming die op 20 maart 2008 plaatsvond, de inzet van de Eerste Kamer daarbij en de reactie van de Minister-President daarop: Handelingen I 2007/08, 31 200 VI, F en Handelingen I 2008/09, nr. 6, blz. 270-271 en 316.)

## 6.2 Bevoegdheden voor het toezicht op de naleving

Het Cbp beschikt over alle bevoegdheden die titel 5.2 van de Awb aan toezichthouders toekent. Op grond van artikel 61, tweede lid, Wbp beschikken collegeleden bovendien over de bevoegdheid tot binnentreden in een woning zonder toestemming van de bewoner. De Algemene wet op het binnentreden is van toepassing. Niet naleven van de medewerkingsplicht, bedoeld in artikel 5:20 Awb, kan worden bejegend met oplegging van een last onder bestuursdwang of een last onder dwangsom.

## 6.3 Bevoegdheden tot bestuursrechtelijke handhaving

Zowel de materiële als de formele bepalingen van de Wbp worden primair met behulp van herstelsancties gehandhaafd. Die keuze is bij de vaststelling van de Wbp gemaakt, mede vanwege het algemeen abstracte karakter van de Wbp. De formulering van veel bepalin-

gen van de Wbp maakt het minder gemakkelijk om het gedrag in concrete situaties af te stemmen op verplichtingen die met punitieve sancties worden bejegend. Die eis vloeit voort uit de eis van voorzienbaarheid bij de wet van artikel 8 EVRM. Het Cbp heeft dan ook op grond van artikel 65 Wbp de bevoegdheid tot het opleggen van een *last onder bestuursdwang* of een *last onder dwangsom*. De procedures zijn geregeld in titel 5.3 van de Awb.
De handhaving van de administratieve verplichtingen (de artikelen 27, 28 en 79 van de Wbp) gebeurt met het opleggen van een *bestuurlijke boete* (artikel 66 Wbp). Het boetemaximum bedraagt momenteel € 4500,=. Ook de protocolplicht in de Wet politiegegevens wordt met een bestuurlijke boete gehandhaafd. De procedures zijn geregeld in titel 5.4 van de Awb. Zowel de hoogte van de bestuurlijke boete als de meer principiële vraag of het belang van de bescherming van persoonsgegevens niet vergt dat het Cbp ook de materiële bepalingen moet kunnen handhaven met punitieve sancties zijn momenteel onderwerp van beraad.

## 6.4 Strafrechtelijke handhaving

Niet naleving van enkele administratieve bepalingen van de Wbp (de artikelen 4, derde lid, 27, 28 en 78, tweede lid, onder a, Wbp) levert een *strafbaar feit* op (artikel 75 Wbp). Het feit is een overtreding. Het strafmaximum is een geldboete van de tweede categorie. Wordt het feit opzettelijk begaan, dan is sprake van een misdrijf. Dan wordt het feit bestraft met een geldboete van de derde categorie of gevangenisstraf van ten hoogste zes maanden. Ook de hoogte van deze straffen is momenteel onderwerp van beraad.

## 6.5 Vormen van intern toezicht

Binnen organisaties, of ze nu tot de overheid of tot het bedrijfsleven behoren, komen verschillende vormen van intern toezicht voor. In alle gevallen is de instelling van intern toezicht in grote mate afhankelijk van de wil van de organisatie daartoe over te gaan. Alleen in uitzonderingsgevallen is er een wettelijke regeling die daartoe verplicht. Dat betekent dat ook de toekenning van taken en bevoegdheden aan interne toezichthouders voornamelijk een kwestie is van intern recht. In de sfeer van de overheid zal daarvoor een *interne regeling* moeten worden vastgesteld. De wetgeving regelt wel de taken en enkele bevoegdheden van de functionaris voor de gegevensbescherming, de privacyfunctionaris en de privacyaudit.

### *6.5.1 Functionaris voor de gegevensbescherming*

Op grond van artikel 62 van de Wbp kan een verantwoordelijke of een organisatie waarbij een verantwoordelijke is aangesloten een *functionaris voor de gegevensbescherming* (FG) benoemen. Zijn taak strekt zich uit tot het uitoefenen van toezicht op de verwerking van persoonsgegevens binnen de organisatie waar hij is benoemd. Hij heeft een vorm van ontslagbescherming die vergelijkbaar is met die van een lid van een ondernemingsraad.

De verantwoordelijke draagt er zorg voor dat de FG beschikt over bevoegdheden die gelijkwaardig zijn aan die van titel 5.2 van de Awb. Verder heeft de FG het recht om de leiding van de organisatie waar hij werkzaam is aanbevelingen te doen. Belangrijke stimulans om tot de aanstelling van een FG over te gaan is dat de meldplicht van verwerkingen kan worden nagekomen door een interne melding aan de FG in plaats van een melding aan het Cbp. Vrijwel alle ministeries hebben een FG aangesteld.

Voorbeelden
Regeling bescherming persoonsgegevens V&W
Regeling toezichtbevoegdheden privacyfunctionaris V&W
Regeling bescherming persoonsgegevens Ministerie VROM
Convenant beveiliging en bescherming persoonsgegevens VROM en VWS (Stcrt. 2003, 118)

Er is geen algemene wettelijke verplichting tot het aanstellen van een FG. Niettemin is het bij de voorbereiding van wettelijke regelingen met betrekking tot de bescherming van persoonsgegevens de moeite waard om te overwegen de aanstelling van een FG voor te schrijven. In een enkel geval heeft de wetgever daartoe besloten.

Voorbeeld
het nieuwe artikel 24g, tweede lid, van de Wet op het onderwijstoezicht, opgenomen in artikel III van het voorstel van wet tot intrekking van de Wet verzelfstandiging informatiseringsbank en wijziging van diverse wetten in verband met de oprichting van de Dienst Uitvoering Onderwijs (DUO) (Kamerstukken II 2008/09, 31 944, nr. 2)

*6.5.2 Privacyfunctionaris*
Artikel 34 van de Wet politiegegevens schrijft de verantwoordelijke voor om een *privacyfunctionaris* aan te stellen. Zijn taak lijkt veel op die van de FG. De verschillen in bevoegdheden van FG en privacyfunctionaris zijn terug te voeren op de afzonderlijke regeling voor de gegevensbescherming ter uitvoering van de politietaak en de structuur van de Wet politiegegevens. De wetgever heeft overigens uitdrukkelijk de mogelijkheid opengelaten dat de verantwoordelijke (of meer verantwoordelijken) in de zin van de Wet politiegegevens ook een FG benoemt met dezelfde taken, ontslagbescherming en bevoegdheden als een FG in zin van de Wbp.

*6.5.3 Privacyaudits*
Geen functionaris maar een controle-instrument is de *privacyaudit*. Ook dit instrument vindt regeling in de Wet politiegegevens. Een privacyaudit is een periodiek onderzoek naar de naleving van een privacyregeling (niet noodzakelijkerwijs een wettelijk voorschrift) door een derde met een zekere onafhankelijkheidswaarborg. Zie artikel 6:5 van het Besluit politiegegevens voor enige details.

*6.5.4 Wettelijke regeling protocolplicht en bewaartermijnen protocolgegevens*
De Wbp kent alleen een algemeen geformuleerde bepaling die betrekking heeft op de kwaliteit van de gegevensverwerking (artikel 11 Wbp). Er bestaat geen zogeheten protocolplicht. Een *protocolplicht* is verplichting om vast te leggen welke handelingen op welk moment met betrekking tot welke persoonsgegevens zijn verricht. Het kan een belangrijk hulpmiddel zijn voor interne en externe toezichthouders en voor de uitoefening van rechten door de betrokkene. Indien aan de protocolplicht ook een bewaartermijn wordt gekoppeld, dient die bewaartermijn ingevolge het arrest van het HvJEG van 7 mei 2009, C-523/07 (Rijkeboer), te worden gerelateerd aan de bewaartermijn van de onderliggende gegevens. Daarbij moet worden bedacht dat sommige gegevens levenslang meegaan.

Voorbeelden
Artikel 32 Wet politiegegevens
Artikelen 19 en 39j Wet justitiële en strafvorderlijke gegevens
Artikel 103 Wet gemeentelijke basisadministratie persoonsgegevens

Advies
Overweeg bij de voorbereiding van wettelijke voorschriften met betrekking tot de bescherming persoonsgegevens of het zinvol is een vorm van intern toezicht te regelen. Dat kan door de benoeming van een functionaris voor de gegevensbescherming of een privacyfunctionaris voor te schrijven. Dat kan aanvullend of alternatief door een privacy-audit of een protocolplicht voor te schrijven.

*6.5.5 Privacy Impact Assessment*
Een Privacy Impact Assessment is een aan een verwerking voorafgaande beoordeling van de effecten die de verwerking heeft op de persoonlijke levenssfeer van betrokkenen, potentiële privacyrisico's te identificeren en de negatieve gevolgen voor betrokkenen én voor verantwoordelijken zoveel mogelijk te beschermen. In de Verenigde Staten wordt dit middel veelvuldig gebruikt bij de voorbereiding van regelgeving. Met de daar gehanteerde methodes is in Nederland nog weinig ervaring opgedaan. Niettemin verdient het aanbeveling, zeker bij uitgebreidere wetsvoorstellen die een groot effect op de bescherming van de persoonlijke levenssfeer kunnen hebben, tevoren de gevolgen voor de persoonlijke levenssfeer in kaart te brengen.

Voorbeeld
Het voorstel Wet kilometerprijs (Kamerstukken II 2009/10, 32 216, nr. 2 en 3)

# 7. De Wbp en andere wetten die informatiebetrekkingen regelen

De Wbp is niet de enige wet waarin informatiebetrekkingen het voornaamste object van de regelgeving zijn. De Wet openbaarheid van bestuur en de Archiefwet 1995 zijn andere belangrijke wettelijke regelingen waarin dergelijke betrekkingen worden geregeld. Bij die wetten gaat het om de toegang van burgers tot informatie die zich onder de overheid bevindt. Bij de voorbereiding van wettelijke regelingen met betrekking tot de bescherming van persoonsgegevens moet onder ogen worden gezien dat deze wetten naast de Wbp van toepassing zijn.
Daarnaast bestaat er een groot aantal wettelijke voorschriften die de burger verplichten informatie, waaronder niet zelden begrepen persoonsgegevens, te verstrekken aan de overheid. Hier gaat het dus om de toegang van de overheid tot informatie die zich bij burgers bevindt. Vaak is de verschaffing van informatie en persoonsgegevens een voorwaarde om voor een prestatie van overheidswege in aanmerking te komen. Tenslotte bestaat er een voor de wetgevingspraktijk én de bestuursrechtelijke praktijk belangrijk grensvlak tussen de Wbp en Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens waar het betreft mogelijkheden tot onderlinge uitwisseling van gegevens. In het onderstaande worden deze wetgevingscomplexen niet inhoudelijk diepgaand behandeld. Wel wordt de verhouding van deze wetgeving tot de Wbp geschetst, voor zover dat voor de wetgeving van belang is. In de wetgevingspraktijk geeft die verhouding regelmatig aanleiding tot vragen.

## *7.1 Wet openbaarheid van bestuur*

*De Wet openbaarheid van bestuur* (Wob) regelt onder welke voorwaarden de overheid bij de uitvoering van zijn taak openbaarheid moet betrachten en in dat belang informatie verstrekt aan het algemene publiek, of de individuele burger. Elke burger heeft het recht een verzoek om informatie, neergelegd in documenten over een bestuurlijke aangelegenheid te richten tot elk bestuursorgaan, of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf (art. 3 Wob). Een verzoek behoort in beginsel te worden ingewilligd. Bestuursorganen dienen daarnaast uit eigen beweging informatie te verschaffen over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering (art. 8 Wob).
Het belang van de burger bij de toegang tot informatie die zich onder de overheid bevindt is een eigenstandig in artikel 110 van de Grondwet erkend belang en is dus noch ondergeschikt, noch bovengeschikt aan het belang van natuurlijke personen bij de bescherming van de hun betreffende gegevens. Het is evident dat die belangen onder omstandigheden onderling tegenstrijdig kunnen zijn. Noch de Wob, noch de Wbp bevatten echter een algemene reikwijdtebepaling die op eenduidige wijze de onderlinge verhouding van beide

wetten regelt. Voor een algemene beschouwing daarover moet worden teruggegrepen op de parlementaire geschiedenis van de Wbp.
Bij de totstandkoming van de Wbp is het uitgangspunt geweest dat de Wob als een lex specialis ten opzichte van de Wbp moest worden aangemerkt (Kamerstukken II 1997/98, 25 892, nr. 3, blz. 42-43). De informatieverplichtingen van de overheid, de artikelen 3 en 8 Wob, golden in de visie van de wetgever dan als uitwerking van de algemene norm van artikel 8, onder c, van de Wbp. Het naleven van de Wob, voor zover het dan betrof de verstrekking van persoonsgegevens, moest als nakoming van een wettelijke verplichting tot gegevensverwerking in de zin van laatstgenoemde bepaling worden aangemerkt.
In de overvloedige rechtspraak over de Wob heeft het uitgangspunt van de wetgever eigenlijk niet echt weerklank gevonden. Blijkbaar kan de praktijk in concrete gevallen goed uit de voeten met de Wob en bestaat daar geen dringende behoefte aan een fundamentele benadering van de verhouding tussen gegevensbescherming en openbaarheid van bestuur. (Vgl. G. Overkleeft-Verburg, Openbaarheid van bestuur, privacywetgeving en gegevensverwerking door de politie, Privacy en Informatie 2007, blz. 194 - 202 en E.J. Daalder, Toegang tot overheidsinformatie, diss. UL, 2005, Den Haag 2005, blz. 204 -206 en 223 - 231.)
Het belang van de bescherming van persoonsgegevens behoort bij de beoordeling van afzonderlijke Wob-verzoeken, én bij afzonderlijke beslissingen van bestuursorganen tot actieve openbaarmaking in concreto in de afweging te worden betrokken. Daarbij gelden de navolgende regels.

*7.1.1 Openbaarmaking bijzondere persoonsgegevens en persoonsidentificerende nummers*
Indien het Wob-verzoek of de voorgenomen beslissing tot actieve openbaarmaking persoonsgegevens betreft als bedoeld in hoofdstuk 2, paragraaf 2, van de Wbp is er sprake van een *absolute weigeringsgrond*. Dit beginsel lijdt slechts uitzondering indien de verstrekking kennelijk geen inbreuk maakt op de persoonlijke levenssfeer (art. 10, eerste lid, onder d, van de Wob). Met nadruk zij erop gewezen dat het hier gaat om de bescherming van *bijzondere persoonsgegevens* in de zin van artikel 16 Wbp én om *persoonsidentificerende nummers* in de zin van artikel 24 Wbp.

*7.1.2 Openbaarmaking andere gegevens*
Indien het Wob-verzoek of de voorgenomen beslissing tot actieve openbaarmaking geen persoonsgegevens betreft als bedoeld in hoofdstuk 2, paragraaf 2, van de Wbp, blijft verstrekking van de gegevens achterwege indien het belang bij verstrekking niet opweegt tegen het belang bij eerbiediging van de persoonlijke levenssfeer; er is dan sprake van een *relatieve weigeringsgrond* (art. 10, tweede lid, onder e, van de Wob).

*7.1.3 Instemming betrokkene met openbaarmaking*
Artikel 10, tweede lid, onder e, van de Wob is niet van toepassing voorzover de betrokkene heeft *ingestemd* met de openbaarmaking (art. 10, derde lid, van de Wob). Deze regel correspondeert met artikel 8, onder a, van de Wbp. Met nadruk zij erop gewezen dat een pendant van artikel 23, eerste lid, onder a, van de Wbp ontbreekt. Dat betekent dat artikel 10, derde lid, van de Wob niet ziet op openbaarmaking van bijzondere persoonsgegevens.

*7.1.4 Verhouding verzoek om openbaarmaking Wob en verzoek om inzage Wbp*
Artikel 3 van de Wob staat naast artikel 35 van de Wbp. Een betrokkene kan zijn persoonsgegevens dus zowel met een *verzoek om openbaarmaking* op grond van de Wob als een *verzoek om inzage* op grond van de Wbp inzien. Uiteraard zijn bedoeling en rechtsgevolgen van beide rechtsmiddelen geheel verschillend.

*7.1.5 Richtsnoeren Cbp*
Het College bescherming persoonsgegevens heeft bij besluit van 13 augustus 2009 de *Richtsnoeren Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer (Stcrt. 12784)* vastgesteld. Deze richtsnoeren geven een gedetailleerd overzicht van de relevante aspecten van de openbaarmaking van gegevens door bestuursorganen op internet.

## 7.2 Archiefwet 1995

*De Archiefwet* 1995 bevat een regeling van de overheidsarchieven. Ook hier betreft het een regeling die erop is gericht zoveel mogelijk informatie openbaar te maken (artikel 14 Archiefwet 1995). Ook bij deze wet kan zich in beginsel een conflict van belangen tussen gegevensbescherming en openbaarheid voordoen. Evenmin als de Wob bevat de Archiefwet 1995 een algemene reikwijdtebepaling die op eenduidige wijze de onderlinge verhouding tussen de Archiefwet 1995 en de Wbp regelt. Bij de voorbereiding van wetgeving die betrekking heeft op de bescherming van de persoonlijke levenssfeer dient men erop bedacht te zijn dat in beginsel alle op grond van de voorgenomen regeling verwerkte persoonsgegevens, voor zover zij ouder zijn dan twintig jaar en zijn neergelegd in archiefbescheiden, worden bestreken door de verplichting dat deze bescheiden hetzij moeten worden overgebracht naar een archiefbewaarplaats, hetzij voor vernietiging in aanmerking komen (artikel 12 Archiefwet 1995).
Het bijhouden van archiefbescheiden door overheidsorganen, de overbrenging naar een archief van persoonsgegevens, en de raadpleging van in archiefbescheiden opgenomen persoonsgegevens zijn vormen van verwerking van persoonsgegevens. Deze verwerking is gerechtvaardigd uit hoofde van artikel 8, onderdelen c en e, van de Wbp. Het bijhouden en toegankelijk maken van in archieven opgenomen persoonsgegevens valt immers aan te merken als een wettelijke verplichting, onderscheidenlijk de vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan.
In artikel 2a van de Archiefwet 1995 is geregeld dat het verbod op het verwerken van bijzondere persoonsgegevens niet geldt voor verwerkingen die verband houden met een

aantal handelingen die als beheersmatige activiteiten met betrekking tot archieven kunnen worden aangemerkt. Dat geldt overigens niet voor het ter raadpleging aanbieden of het ter gebruik beschikbaar stellen van archiefbescheiden. De wetgever heeft erkend dat de bescherming van de persoonlijke levenssfeer een belang is op grond waarvan de openbaarheid van naar een archiefbewaarplaats overgebrachte archiefbescheiden kan worden beperkt (artikel 15, eerste lid, onder a, van de Archiefwet 1995). De beslissing daartoe berust niet bij de archiefbewaarder, maar bij de "zorgdrager" in de zin van de Archiefwet 1995. Niet zelden zal die hoedanigheid samenvallen met die van verantwoordelijke in de zin van de Wbp.
Verzoeken om inzage op grond van artikel 35 Wbp staan naast verzoeken om raadpleging van archiefbescheiden. De inwilliging van verzoeken om correctie op grond van artikel 36 van de Wbp gebeurt niet door verwijdering of vernietiging van gegevens, maar door toevoeging van een lezing van betrokkene aan de archiefbescheiden. Ingevolge artikel 44, tweede lid, Wbp kan de transparantieverplichting buiten toepassing worden gelaten ten aanzien van persoonsgegevens die zijn opgenomen in bescheiden die naar een archiefbewaarplaats zijn overgebracht.

Advies

Bij de voorbereiding van wetgeving met betrekking tot de bescherming van persoonsgegevens moet onder ogen worden gezien dat de Wet openbaarheid van bestuur en de Archiefwet 1995 naast de Wbp blijven gelden.

## *7.3 Verplichtingen tot informatieverschaffing*

De formele wetgever heeft in veel gevallen verplichtingen in het leven geroepen tot het verschaffen van informatie aan bestuursorganen. Niet zelden impliceert de verschaffing van informatie dat het desbetreffende bestuursorgaan persoonsgegevens gaat verwerken, veelal in de vorm van verzamelen of doorgeven. Er zijn twee typen verplichtingen tot informatieverschaffing te onderscheiden. Het eerste type is de verplichting tot het verschaffen van informatie door burgers en bedrijven aan de bestuursorganen. Het tweede type is de verplichting tot verstrekking van informatie tussen bestuursorganen onderling.
Wanneer het inderdaad de bedoeling is dat informatieverschaffing (mede) tot doel heeft persoonsgegevens te verzamelen of over te dragen, moet de desbetreffende bepaling in ieder geval in overeenstemming met de artikelen 6, 7, 8 en 9 van de Wbp worden geredigeerd. Wanneer de noodzaak zich aandient om buiten redelijke twijfel te stellen dat gegevens door de juiste persoon worden opgegeven, kan oplegging van een identificatieplicht worden overwogen. Daarvoor is een wettelijke voorziening nodig. Die voorziening moet conform de *Wet op de identificatieplicht* worden vormgegeven. De noodzaak voor de voorziening moet in de memorie van toelichting worden onderbouwd. Wanneer het de bedoeling is dat (mede) bijzondere persoonsgegevens worden overgedragen, dan moet de

bepaling daarvoor een uitdrukkelijke wettelijke grondslag bevatten, voor zover de Wbp daarin niet expliciet voorziet. Zie daarvoor nader de paragrafen 4.7, 4.8, 5.2 en 5.4.

Voorbeelden gegevensverzameling

Artikel 47 Algemene wet inzake rijksbelastingen
Artikelen 17 en 53a Wet werk en bijstand
Artikel 2 van de Wet op de identificatieplicht

Voorbeelden gegevensverstrekking

Artikel 67 Wet werk en bijstand
Artikelen 107 en 107a van de Vreemdelingenwet 2000
Artikel 54 Wet structuur uitvoeringsorganisatie werk en inkomen

## *7.4 Wet justitiële en strafvorderlijke gegevens en Wet politiegegevens - informatiehuishouding openbaar ministerie en politie*

In deze leidraad kan niet uitgebreid worden ingegaan op de wetten die de informatiehuishouding van openbaar ministerie en politie regelen. Om twee redenen wordt toch kort ingegaan op de positie van openbaar ministerie en politie. De eerste is dat de Wbp van toepassing blijft op enkele taken van beide organisaties. De tweede is dat op grond van de Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens beleid, respectievelijk regels, zijn vastgesteld over de verstrekking van gegevens afkomstig van openbaar ministerie en politie aan samenwerkingsverbanden met derde partijen.

### *7.4.1 Wet justitiële en strafvorderlijke gegevens - openbaar ministerie*

De informatiehuishouding van het openbaar ministerie valt voor zijn strafrechtelijke taken geheel onder de werking van de *Wet justitiële en strafvorderlijke gegevens (Wjsg)*. Het openbaar ministerie verwerkt op grond van de Wsjg zowel justitiële als strafvorderlijke gegevens. Voor de gegevensverwerking verband houdend met de taken die het openbaar ministerie op privaatrechtelijk terrein vervult, valt het OM onder de werking van de Wbp. Op grond van artikel 39f, eerste lid, van de Wjsg kan het College van procureurs-generaal voor zover dit noodzakelijk is in een zwaarwegend algemeen belang aan personen of instanties, ten behoeve van een aantal nader bepaalde doelen strafvorderlijke gegevens verstrekken. Deze bevoegdheid van het College is van bijzonder belang voor *samenwerkingsverbanden* waarin het openbaar ministerie met derde partijen participeert. De wijze waarop die bevoegdheid wordt uitgeoefend is neergelegd in de *Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (aanwijzing wet justitiële en strafvorderlijke gegevens) van 28 januari 2008 (Stcrt. 19)*.

De geheimhoudingsbepaling van artikel 52 Wjsg legt overigens strenge beperkingen op aan de mogelijkheden aldus verstrekte gegevens verder te verwerken.

*7.4.2 Wet politiegegevens - politie, Koninklijke marechaussee, bijzondere opsporingsdiensten*

De informatiehuishouding van de politie en de Koninklijke marechaussee valt, voor zover deze organisaties gegevens verwerken ter uitvoering van de politietaak, bedoeld in de artikelen 2 en 6 Politiewet 1993, onder de werking van de *Wet politiegegevens* (Wpolg). Onder de politietaken worden ook de zogenoemde taken ten dienste van de justitie, bedoeld in artikel 1, onder g, van de Politiewet 1993 gerekend. Uit de reikwijdtebepaling van art. 2, tweede lid, onder c, van de Wbp volgt dat het gaat om alle vormen van gegevensverwerking ten behoeve van de politietaak, dus ook wanneer het een verwerking betreft die geen specifieke regeling vindt in de Wet politiegegevens. Wanneer de politie optreedt als *toezichthouder in de zin van afdeling 5.2 van de Algemene wet bestuursrecht* valt de verwerking van persoonsgegevens in het kader van toezichthoudende activiteiten wel onder de reikwijdte van de Wbp.

Op grond van artikel 20 Wpolg kan de verantwoordelijke voor de gegevensverwerking voor zover dit noodzakelijk is in een zwaarwegend maatschappelijk belang ten behoeve van een *samenwerkingsverband* van de politie met personen of instanties, in overeenstemming met het bevoegd gezag, ten behoeve van een aantal nader bepaalde doelen politiegegevens verstrekken.

Het *Besluit politiegegevens* bevat een uitgewerkte regeling voor de verstrekking van politiegegevens. Zie ook de *regeling van de Minister van Justitie van 1 februari 2008, nr. 5528485/08, houdende regels tot het aanwijzen van wetgeving, genoemd in artikel 4:2, tweede lid, van het Besluit politiegegevens (Stcrt. 38)*.

*Het Besluit politiegegevens bijzondere opsporingsdiensten* regelt de verstrekking van politiegegevens afkomstig uit verwerkingen door de bijzondere opsporingsdiensten in de zin van de *Wet op de bijzondere opsporingsdiensten*. Dat betekent dat de desbetreffende verwerkingen niet meer zijn onderworpen aan het regime van de Wbp, ook al geschiedt dit onder verantwoordelijkheid van de voor de bijzondere opsporingsdienst verantwoordelijke minister.

# 8. Procedurele aspecten

## 8.1 Overleg met het Ministerie van Justitie

Bij de voorbereiding van regelgeving waarin aspecten met betrekking tot de bescherming van persoonsgegevens regeling vinden, is het onder bepaalde omstandigheden aan te raden contact te zoeken met de directie Wetgeving van het Ministerie van Justitie. Zeker bij meer omvangrijke of ingewikkelde wetsvoorstellen is het verstandig dit contact tijdig te leggen. Tijdig wil zeggen: voorafgaand aan de formele aanbieding van een voorstel voor de wetgevingstoets. Op die manier wordt voorkomen dat een behandeling van een wetsvoorstel in een voorportaal of onderraad nodeloos vertraging oploopt omdat er nog geen overeenstemming met Justitie is over het onderwerp gegevensbescherming. Contacten kunnen zonodig worden gelegd via de toetser van de sector Wetgevingskwaliteitsbeleid van de directie Wetgeving van het Ministerie van Justitie die de wetgeving van het desbetreffende ministerie toetst.
Overleg met het Ministerie van Justitie is in elk geval noodzakelijk in de navolgende gevallen:

- voornemens om uitdrukkelijke afwijkingen van de Wbp tot stand te brengen
- voornemens tot regelgeving met betrekking tot de verwerking van bijzondere persoonsgegevens die buiten het kader van de artikelen 16 tot en met 23 Wbp treden
- voornemens tot regelgeving waarbij een uitdrukkelijk beroep wordt gedaan op de exceptie van artikel 23, eerste lid, onder e, van de Wbp
- voornemens tot regelgeving met betrekking tot nieuwe persoonsidentificerende nummers
- voornemens om toezicht op de naleving of bestuursrechtelijke handhaving van regels met betrekking tot de bescherming van persoonsgegevens in bijzondere wettelijke regelingen (mede) op te dragen aan andere toezichthouders c.q. bestuursorganen dan het Cbp

Verder is het gewenst het overleg met het Ministerie van Justitie aan te gaan bij:

- voorstellen tot aanpassing van het Vrijstellingsbesluit Wbp
- voorstellen tot aanpassing van het Besluit gebruik sofi-nummer Wbp

## 8.2 Advisering College bescherming persoonsgegevens

*8.2.1 Wetgevingsadvisering*
Op grond van artikel 51, tweede lid, van de Wbp wordt het Cbp om advies gevraagd over *wetsvoorstellen en ontwerpen van algemene maatregel van bestuur* die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. In de jaren ‘90 van de twintigste eeuw zijn wettelijke adviesverplichtingen voor een belangrijk deel afgeschaft. Artikel 51 Wbp is echter gehandhaafd, omdat zij voortvloeit uit het Europese recht. Artikel

28, tweede lid, van richtlijn nr. 95/46/EG schrijft een dergelijke verplichting voor. Het nalaten aan deze verplichting te voldoen betekent dus dat niet slechts in strijd met de wet, maar ook in strijd met Europees recht wordt gehandeld. Onder omstandigheden zou dat voor de Europese Commissie aanleiding kunnen zijn voor het starten van een inbreukprocedure.

Uit de bewoordingen van artikel 51, tweede lid, van de Wbp kan wel worden afgeleid dat de verplichting slechts geldt ten aanzien van wetgeving die *geheel of voor een belangrijk deel* betrekking heeft op de verwerking van persoonsgegevens. Het laatste criterium zal in afzonderlijke gevallen ongetwijfeld wel eens de vraag oproepen of de verplichting wel geldt. Artikel 51, tweede lid, Wbp moet materieel worden ingevuld. Het gaat niet om het tellen van afzonderlijke bepalingen.
Wanneer er sprake is van een ontwerpregeling die grotendeels uit bepalingen bestaat waarin geen aspecten betreffende de verwerking van persoonsgegevens zijn geregeld - bijvoorbeeld omdat veel andere regelingen wetgevingstechnisch moeten worden aangepast - maar de regeling in materiële zin wel gaat om het gebruik van persoonsgegevens als overheidsinterventie, of waarin de bescherming van die gegevens bijzondere aandacht krijgt, moet er advies aan het Cbp worden gevraagd, ook al betreft het misschien een gering aantal bepalingen. Hetzelfde geldt voor regelingen waarin aanvullingen of afwijkingen van de Wbp zijn opgenomen.
Verder geldt de verplichting advies te vragen niet ten aanzien van *regelende kleine koninklijke besluiten, ministeriële regelingen of beleidsregels* die betrekking hebben op onderwerpen van gegevensbescherming. Uiteraard kan het onder omstandigheden toch verstandig zijn een advies aan het Cbp te verzoeken over ontwerpen voor deze categorieën regelingen.

Het Cbp brengt ook verplicht wetgevingsadvies uit bij wijzigingen van de *Wet politiegegevens* (artikel 35, tweede lid, Wet politiegegevens), de *Wet justitiële en strafvorderlijke gegevens* (artikel 27, tweede lid, Wet justitiële en strafvorderlijke gegevens) en de *Wet gemeentelijke basisadministratie persoonsgegevens* (artikel 120, derde lid, Wet gemeentelijke basisadministratie persoonsgegevens) en op een enkel onderdeel van het *Wetboek van Strafvordering*. Het Cbp heeft geen adviesbevoegdheid ten aanzien van de Wet op de inlichtingen- en veiligheidsdiensten 2002.
Wetgevingsadviezen kunnen op grond van de *Kaderwet adviescolleges* ook door de beide Kamers der Staten-Generaal worden gevraagd aan het Cbp. De Kamers behoren dat wel te doen met inachtneming van de door de wetgever geregelde materiële adviesbevoegdheid van het desbetreffende adviesorgaan.
Uit artikel 24 van de Kaderwet adviescolleges en uit aanwijzing 213 van de Aanwijzingen voor de regelgeving vloeit voort dat op een advies van het Cbp expliciet wordt gereageerd in de memorie van toelichting, zeker wanneer een advies geheel of gedeeltelijk niet wordt gevolgd.

*8.2.2 Andere vormen van advisering*
Het Cbp heeft buiten de wetgevingsadvisering geen andere uitdrukkelijke wettelijke adviestaken. In het verleden werd het Cbp dikwijls om beleidsadviezen gevraagd of gevraagd voorlichting in algemene zin te geven over de oplossing van problemen op het

gebied van de gegevensbescherming. Daarvoor is nu in beginsel geen ruimte meer. Wat de advisering betreft moet het Cbp zich concentreren op de wetgevingsadvisering. Voor het overige moet het Cbp zijn taak als toezichthouder en handhaver vervullen. Het Cbp wil zich vooral op die laatste taken richten. Het geven van andere dan wetgevingsadviezen kan gemakkelijk interfereren met de toezichthoudende en handhavende taak.

# 9. Lijst van modelbepalingen

## *9.1 Modelbepalingen*

*Modelbepaling verwijzing naar begrippen Wbp*

In deze wet (en de daarop berustende bepalingen) wordt verstaan onder: persoonsgegevens, verwerking van persoonsgegevens, bestand, verantwoordelijke, bewerker, onderscheidenlijk betrokkene, hetgeen daaronder wordt verstaan in artikel 1 van de Wet bescherming persoonsgegevens.

*Modelbepaling doelomschrijving en aanwijzing verantwoordelijke*

Ten behoeve van (opsomming doeleinden of verwijzing naar een andere bepaling waarin de doeleinden zijn beschreven) worden persoonsgegevens verwerkt. (Bestuursorgaan) is verantwoordelijke voor deze verwerking.

*Modelbepalingen gegevensverstrekking*

Variant I

1. (Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken andere bestuursorganen de gegevens betreffende (doelomschrijving en betrokkenen aanduiden) welke zij behoeven voor de uitvoering van hun taak.
2. Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.
3. De in het eerste en tweede lid bedoelde gegevensverstrekking vindt niet plaats indien de persoonlijke levenssfeer van de betrokkene daardoor onevenredig wordt geschaad.

of

Variant II

1. (Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken andere bestuursorganen de navolgende gegevens welke zij behoeven voor de uitvoering van hun taak:

a.(...)
b.(...)
c.(...) etc.

2. Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.

of

Variant III

1. (Naam bestuursorgaan of bestuursorganen), onderscheidenlijk een bij of krachtens deze wet aangewezen toezichthouder, verstrekken (naam bestuursorgaan of bestuursorganen) de navolgende gegevens ten behoeve van de goede uitvoering van (citeertitel of aanhaling regeling):

a.(...)
b.(...)
c.(...) etc.

2. Andere bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht aan (naam bestuursorgaan of bestuursorganen) de gegevens te verstrekken die noodzakelijk zijn voor de uitvoering en het toezicht op de naleving van deze wet.

*Facultatieve bepalingen*

4 (of 3). Onverminderd artikel 10 van de Wet algemene bepalingen burgerservicenummer kunnen de bestuursorganen, bedoeld in het eerste en tweede lid, bij de verstrekking van gegevens op grond van het eerste of tweede lid gebruik maken van (omschrijving persoonsidentificerend nummer, anders dan het burgerservicenummer).

5 (of 4). Bij algemene maatregel van bestuur worden regels gesteld omtrent de gevallen waarin en de wijze waarop in ieder geval gegevens dienen te worden verstrekt.

6 (of 5). Bij de verstrekking van gegevens op grond van het eerste of tweede lid kunnen slechts bijzondere persoonsgegevens als bedoeld in artikel 16 van de Wet bescherming persoonsgegevens worden verstrekt, voor zover deze gegevens noodzakelijk zijn voor (doelomschrijving).

7(of 6). De gegevens, bedoeld in het voorgaande lid, worden verwerkt door (naam bestuursorgaan en/of toezichthouder dat/die als verantwoordelijke(n) word(t)(en) aangewezen). Zij kunnen slechts worden verwerkt door derden, voor zover deze betrokken zijn bij de uitvoering van deze wet en daartoe noodzakelijkerwijs de beschikking over deze gegevens verkrijgen.

8 (of 7). Bij algemene maatregel van bestuur/ regeling van Onze Minister worden regels gesteld ter waarborging van de persoonlijke levenssfeer. Daarbij wordt in elk geval geregeld:

a. op welke wijze de verwerking bedoeld in het zesde (of vijfde) lid, plaatsvindt;
b. op welke wijze door passende technische en organisatorische maatregelen deze gegevens worden beveiligd tegen verlies of onrechtmatige verwerking;
c. welke gegevens, aan welke personen of instanties, voor welk doel en op welke wijze kunnen worden verstrekt;
d. op welke wijze wordt gewaarborgd dat de verwerkte persoonsgegevens slechts worden verwerkt voor het doel waarvoor zij zijn verzameld of voor zover het verwerken met dat doel verenigbaar is, alsmede hoe daarop wordt toegezien.

9 (of 8). (Naam bestuursorgaan) benoemt een functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de Wet bescherming persoonsgegevens/ een privacyfunctionaris die toeziet op de verwerking van persoonsgegevens krachtens het eerste/ krachtens het eerste en tweede lid.

# Trefwoordenregister

# Register op bepalingen van de Wet bescherming persoonsgegevens