

AAN Minister van Binnenlandse Zaken en
Koninkrijksrelaties

Postbus 20011
2500 EA DEN HAAG

DATUM 5 maart 2013

ONS KENMERK z2012-00847

CONTACTPERSOON

UW BRIEF VAN 4 december 2012

UW KENMERK

ONDERWERP Advies – concept Toetsmodel Privacy Impact
Assessment

Geachte ,

Bij brief van 4 december 2012 verzoekt u het College bescherming persoonsgegevens (CBP) te adviseren over het *Toetsmodel Privacy Impact Assessment* (PIA) (hierna: concept-toetsmodel). Dit nieuwe instrument houdt nauw verband met de wettelijke adviestaak in artikel 51, lid 2, van de Wet bescherming persoonsgegevens (Wbp) van het CBP.

Het CBP constateert met grote instemming dat er uitvoering wordt gegeven aan de motie-Franken, waardoor een PIA standaard gebruikt zal worden bij de totstandkoming van wetgeving en/of beleidsstukken. Voor het CBP is het belangrijk dat verantwoordelijken middels een PIA worden gestimuleerd om zich bewust te zijn van, en verantwoordelijkheid te nemen voor een zorgvuldige verwerking van persoonsgegevens. Zodoende wordt het initiatief om te komen tot een PIA zeer positief gewaardeerd door het CBP.

In hoofdlijnen wil het CBP echter nog het volgende meegeven. Een PIA is geen "compliance toets," maar een instrument om in een zeer vroegtijdig stadium van de ontwikkeling van nieuwe producten, diensten en beleidsvoornemens aan allen die daar mee doende zijn en aan leidinggevendenden de risico's in relatie tot bescherming persoonsgegevens op overzichtelijke wijze in kaart te brengen. Met die kennis gewapend kan vervolgens de verdere ontwikkeling van het product, de dienst of het beleidsvoornemen ter hand genomen worden en kan de meer juridische "compliance" toets (d.w.z. voldoet het voornemen in uitwerking aan, met name, de Wbp) verricht worden. In het voorliggende concept-toetsmodel worden de begrippen "compliance toets" en de "PIA-toets" soms met elkaar verward. Reden om daar langs deze weg nadrukkelijk aandacht voor te vragen.

Het CBP geeft u in overweging om de punten uit dit advies (zie: bijlagen) mee te nemen bij de uiteindelijke implementatie van het concept-toetsmodel.

DATUM 5 maart 2013
ONS KENMERK z2012-00847

Voor het volledige advies verwijs ik u naar de bijlagen bij deze brief. Indien gewenst kan dit advies op ambtelijk niveau nader toegelicht worden.

Voor een nadere toelichting op het advies ben ik ook graag beschikbaar.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

Het advies van het College bescherming persoonsgegevens van 5 maart 2013 over het concept Toetsmodel Privacy Impact Assessment (z2012-00847)

Bij brief van 4 december 2012 verzoekt de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het College bescherming persoonsgegevens (CBP) te adviseren over het *Toetsmodel Privacy Impact Assessment* (PIA) (hierna: concept-toetsmodel). Aangezien het nieuwe instrument nauw verband houdt met de wettelijke adviestaak in artikel 51, lid 2, van de Wet bescherming persoonsgegevens (Wbp) van het CBP stelt de minister van BZK een advies zeer op prijs.

Achtergrond

In oktober 2009 heeft het College bescherming persoonsgegevens (CBP) het initiatief genomen om in samenwerking met het bedrijfsleven en de overheid (waaronder BZK) een PIA te ontwikkelen (z2009-00773) (hierna: concept-PIA 2009-2010). De toenmalige minister van Justitie heeft in een brief aan de Tweede Kamer van 3 november 2009¹ enthousiast mededeling gedaan van dit initiatief. In november 2010 heeft het CBP zijn betrokkenheid bij het ontwikkelen van deze gezamenlijke PIA beëindigd. Redenen daarvoor waren onder meer dat de weliswaar getoonde betrokkenheid niet leidde tot de gewenste voortvarendheid waarmee tot de daadwerkelijke ontwikkeling werd gekomen, het terugtrekken van een grote samenwerkingspartner en de intentie van verschillende leden om zelfstandig op andere wijze en meer specifiek voor hun eigen sector te komen tot een PIA. Het CBP was ten aanzien van het laatste punt van oordeel dat daarmee recht werd gedaan aan de overtuiging van het CBP dat de verantwoordelijkheid voor een zorgvuldige omgang met persoonsgegevens (en afgeleid daarvan voor de ontwikkeling van een PIA) primair ligt bij diegene die deze persoonsgegevens verwerkt.

De belangrijkste aandachtspunten van deze concept-PIA 2009-2010 waren:

- Het is belangrijk om in het hele PIA-instrument eenvoudige, toegankelijke taal te gebruiken, zonder jargon, zodat de PIA ook begrijpelijk is voor mensen zonder juridische of ICT-achtergrond. Dit is een aandachtspunt voor de hele PIA.
- De PIA dient zich niet alleen te richten op de grotere verwerkingen/organisaties (met interne expertise en/of middelen om experts in te huren) maar ook op kleinere organisaties met eenvoudige verwerkingen.
- De PIA moet zo geschreven worden dat het duidelijk is dat het uitvoeren van de PIA op zichzelf een duidelijk resultaat oplevert, namelijk: dat de gebruiker na het invullen van de PIA-vragenlijst weet waar bij zijn project de privacyrisico's zitten. In het toentertijd ontwikkelde concept-PIA werd op veel plaatsen nog verwezen naar privacy experts en andere privacy instrumenten. Dit zal bepaalde gebruikers afschrikken en leidt af van de resultaten van de PIA.

Inhoud concept-toetsmodel²

Tijdens het beleidsdebat over privacy in de Eerste Kamer in mei 2011 is de motie-Franken aangenomen. Daarin wordt de regering verzocht om bij ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een zogenaamde PIA.³ In het regeerakkoord is

¹ Kamerstukken II 2009-2010, 31 051, nr. 5.

² Zie: begeleidende brief van de minister van BZK van 6 december 2012 bij het concept-toetsmodel.

³ Kamerstukken II 2010-2011, 31 050, D

vervolgens aangekondigd dat standaard een PIA gebruikt moet worden. Het afgelopen jaar is interdepartementaal een concept-toetsmodel voor de uitvoering van een PIA ontwikkeld. Het is de bedoeling standaard toepassing hiervan te bewerkstelligen door opname ervan in het Integraal Afwegingskader voor Beleid en Regelgeving (IAK).

Juridisch kader

Het CBP toetst wetsvoorstellen in beginsel aan artikel 10 van de Grondwet, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en aan de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, waarvan de Wbp een uitwerking is. Het thans voorliggende concept-toetsmodel is echter geen wetsvoorstel in de zin van artikel 51 lid 2 Wbp, maar een nieuw toetsinstrument op beleidsniveau dat nauw verband houdt met de wettelijke adviestaak van het CBP. Gezien het feit dat het concept-toetsmodel is voortgekomen uit de motie-Franken en het CBP al eerder een concept-PIA in 2009-2010 (reeds in uw bezit) heeft geïnitieerd⁴, zullen deze documenten het toetsingskader vormen voor dit advies.

Het CBP zal het thans voorliggende concept-toetsmodel dan ook toetsen aan deze documenten, waarbij ook rekenschap wordt gegeven van de eerdere ervaringen van het CBP ten aanzien van wetgevingsadvisering.

Grondbeginselen PIA

Het CBP verstaat onder een PIA het volgende.⁵

1. PIA is een instrument om privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in beeld te kunnen brengen.
2. De PIA stimuleert organisaties om proactief na te denken over vragen als:
 - a. Wat is de impact van het beoogde project op de privacy van betrokkenen?
 - b. Wat zijn de risico's voor de betrokkenen en voor de organisatie?
 - c. Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk, gegeven de doelstellingen van het project?
3. Na het uitvoeren van de PIA kan de verantwoordelijke gerichte opdrachten geven aan degene die het product of dienst verder ontwikkelt opdat maatwerk kan worden geleverd en wordt voorkomen dat in een later stadium kostbare aanpassingen nodig zijn.
4. De PIA kan onderdeel worden van de privacystrategie en het kwaliteitssysteem van een organisatie of van de kwaliteitsbewaking van een project.
5. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

Beoordeling

Het CBP constateert met instemming dat er uitvoering wordt gegeven aan de motie-Franken, waardoor een PIA standaard gebruikt zal worden bij de totstandkoming van wetgeving en/of beleidsstukken. Voor het CBP is het belangrijk dat verantwoordelijken middels een PIA worden

⁴ Zie: "a. Achtergrond", p. 6 en 8-9.

⁵ Zie: concept-PIA 2009-2010, p. 6 en 8-9.

gestimuleerd om zich bewust te zijn van, en verantwoordelijkheid te nemen voor een zorgvuldige verwerking van persoonsgegevens. Zodoende wordt het initiatief om te komen tot een PIA positief gewaardeerd door het CBP. Ten aanzien van de uitwerking geeft het CBP graag de volgende suggesties mee.

1. PIA: wanneer en noodzaak

In het concept-toetsmodel⁶ is een hoofdstuk opgenomen over wanneer een PIA uitgevoerd kan worden. Uit dit hoofdstuk wordt echter niet voldoende duidelijk op welk specifiek moment een PIA uitgevoerd dient te worden.

In de motie-Franken staat vermeld dat bij de totstandkoming van nieuwe wetgeving uitdrukkelijk aandacht moet worden gegeven aan de vraag of de beperkingen op het grondrecht tot bescherming van de persoonlijke levenssfeer gerechtvaardigd zijn en dat voor de beantwoording van deze vraag getoetst dient te worden aan onder meer de resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico's de maatregel met zich meebrengt. Uit de grondbeginselen van een PIA kan opgemaakt worden dat het een instrument is waarmee vroegtijdig de privacyrisico's op een gestructureerde en heldere manier naar voren gebracht kunnen worden. Het "Handbook Information Commissioner's Office" (ICO) geeft nadere invulling aan de term "vroegtijdig." Het "Handbook ICO" geeft het advies om in de initialisatiefase van het project een PIA uit te voeren.⁷

Daarnaast kan beleidsvoorbereiding getypeerd worden als een dynamisch proces. In concept-PIA 2009-2010 (p. 10) staat ook vermeld dat wanneer de omstandigheden van een project tijdens een looptijd veranderen, het raadzaam is om de PIA te herhalen. Het uitvoeren van een PIA is daarmee geen statisch, maar een cyclisch proces. Daarmee dient dus ook de noodzaak opnieuw belicht te worden, hetgeen het belangrijkste beginsel is van de Wbp, zoals Wilbert Tomesen (collegelid CBP) onder meer tijdens het rondetafelgesprek met de tijdelijke commissie ICT van de Tweede Kamer op 21 januari 2013 heeft uitgesproken.⁸ Bij wetgevingsadvisering toetst het CBP wetgeving ook primair aan de vraag of het verwerken van de persoonsgegevens noodzakelijk is. Ook de motie-Franken geeft de noodzaak aan als een van de belangrijke criteria om rekening mee te houden bij de totstandkoming van nieuwe wetgeving.

Het CBP geeft in overweging om - op basis van het voorgaande - in het hoofdstuk "Wanneer" van het concept-toetsmodel meer richting te geven aan het moment of de momenten waarop de beleidsmaker of wetgevingsjurist een PIA dient uit te voeren. Ook adviseert het CBP om de noodzaak van gegevensverwerking explicieter mee te nemen in het dynamische wetgevings- en beleidsadviseringsproces.

⁶ Zie: pagina 2-3

⁷ URL: http://www.ico.gov.uk/pia_handbook_html_v2/html/1-Chap1-4.html

⁸ Verder is het volgende aangegeven: "(...) de eindverantwoordelijkheid voor de naleving van het grondrecht op een zo hoog mogelijk bestuurlijk niveau moeten worden belegd. De privacywetgeving is in essentie terug te brengen tot de volgende drie principes:

a) Noodzaak: verzamel niet meer persoonsgegevens dan noodzakelijk voor het vastgestelde doel en bewaar ze niet langer dan noodzakelijk voor het doel; b) Transparantie: informeer de betrokkenen - van wie de gegevens zijn - waartoe deze gegevens worden verzameld en gebruikt; c) Beveiliging: zorg voor een adequate beveiliging van de gegevens."

2. Risico's

Het concept-toetsmodel vermeldt dat deze richtinggevend en corrigerend⁹ bedoeld is. Uit PIA 2009-2010 kan opgemaakt worden dat een PIA een instrument is om privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in beeld te kunnen brengen.

Het concept-toetsmodel geeft nog onvoldoende handvatten aan de beoordelaars. De antwoorden die op basis van de PIA kunnen worden gegeven (ja/nee) krijgen geen verdere toelichting. Hierdoor geeft het de beoordelaar onvoldoende aanknopingspunten om de privacy risico's van het beoogde project voor de betrokkenen in te schatten en welke alternatieve mogelijkheden er zijn. (zie: grondbeginselen PIA nrs. 1, 2) (zie ook: motie-Franken).

Het thans voorliggende concept-toetsmodel kan de verantwoordelijke onvoldoende van hulp voorzien bij ontwikkeling van beleid en wetgeving, waarbij de implicaties voor gegevensbescherming op gestructureerde en transparante wijze in kaart zouden moeten worden gebracht. Het CBP adviseert om het concept-toetsmodel te voorzien van een duidelijke toelichting ten aanzien van onder meer de impact.

3. Samenhang Leidraad

Het is onduidelijk wat de samenhang en/of meerwaarde is van het thans voorliggende concept-toetsmodel boven de *Leidraad – afstemmen van wetgeving op de Wet bescherming persoonsgegevens* dat in 2010 is uitgegeven door de toenmalige minister van Justitie. Deze leidraad is – evenals het concept-toetsmodel – bedoeld voor wetgevingsjuristen werkzaam op de wetgevingsafdelingen van de ministeries, de Raad van State en beleidsambtenaren.¹⁰ Beide documenten zijn juridisch van aard.

Een PIA is in beginsel geen juridische controle (daarvoor kan aldus de reeds bestaande *Leidraad – afstemmen van wetgeving op de Wet bescherming persoonsgegevens* gebruikt worden), maar zou een diepgaandere en bredere controle dienen te omvatten. Het concept PIA 2009¹¹ en het "Handbook ICO" geven bovendien aan dat na het uitvoeren van een PIA een compliance toets (ofwel: juridische controle) uitgevoerd kan worden. Het thans voorliggende concept-toetsmodel heeft eerder de contouren van een compliance toets dan van een PIA, vanwege het feit dat het concept-toetsmodel hoofdzakelijk de Wbp-artikelen naloop en daarmee dus eerder een juridische controle omvat.

Het CBP adviseert de minister om het concept-toetsmodel aan te passen, zodat het onderscheid tussen een PIA en de *Leidraad – afstemmen van wetgeving op de Wet bescherming persoonsgegevens* duidelijk wordt.

⁹ Zie: het concept-toetsmodel, p. 1.

¹⁰ Zie: *Leidraad – afstemmen van wetgeving op de Wet bescherming persoonsgegevens*, p 9.

¹¹ Zie: Concept PIA 2009-2010, p. 10.

4. Status PIA

In de begeleidende brief staat dat het concept-toetsmodel onderdeel uit gaat maken van het IAK. Op de website van het IAK¹² staat het volgende vermeld: “Het IAK is een werkwijze en een kennisbank voor het voorbereiden en verantwoorden van beleids- en wetgevingsvoorstellen. Met het afwegingsdossier kunnen beleidsmedewerkers en wetgevingsjuristen bij de Rijksoverheid het IAK toepassen bij het voorbereiden van een beleids- of wetgevingsvoorstel” (onderstreping toegevoegd door het CBP).

Hiermee lijkt (zie onderstreping in het hierboven geciteerde cursieve gedeelte) dat het uitvoeren van een PIA een mogelijkheid is, terwijl in de motie-Franken vermeld staat “(...) bij de tot stand brengen van nieuwe wetgeving uitdrukkelijk aandacht moet worden gegeven aan de vraag of de beperking op het grondrecht tot bescherming van de persoonlijke levenssfeer gerechtvaardigd zijn, overwegende, dat voor de beantwoording van deze vraag aansluitend aan de verdragsverplichting moet worden getoetst aan de volgende criteria: (...) 3. De resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico's de maatregel met zich meebrengt, (...)” (onderstreping toegevoegd door het CBP).

Het CBP adviseert om deze discrepantie meer in lijn te brengen met de motie-Franken.

5. Verantwoordingsparagraaf

In het concept-toetsmodel wordt het volgende voorbeeld van een volledig gestandaardiseerde verantwoordingsparagraaf gegeven, dat een modelement van deze MvT-paragraaf zou kunnen zijn:

“Gezien de aard van dit voorstel is in de fase van beleidsontwikkeling een Privacy Impact Assessment uitgevoerd (zie ook Kamerstukken I, 2012/2011, 31051, nr. D; motie Franken). Met behulp hiervan zijn op gestructureerde wijze de implicaties van de maatregel(en)/het systeem op gegevensbescherming in kaart gebracht. Hierbij is in het bijzonder aandacht besteed aan de beginselen van gegevensminimalisering en doelbinding, het vereiste van een goede beveiliging en de rechten van betrokkenen. [Beschrijving specifieke aspecten].”

Dit modelement geeft aan dat er een PIA is geweest en welke elementen daarbij aan bod zijn gekomen. Het CBP mist bij de opsomming van de derde volzin dat er ook bijzonder aandacht besteed moet worden aan de noodzaak. Het CBP adviseert om de noodzaak toe te voegen aan de opsomming.

Het CBP adviseert voorts om de “beschrijving specifieke aspecten” te vervangen en/of aan te vullen met de “specifieke belangenafwegingen” die gemaakt zijn tijdens een PIA. In dit onderdeel zal dan de op maat gesneden belangenafweging beschreven kunnen worden.

Het CBP adviseert om de PIA onder meer conform de motie-Franken uitgebreider te beschrijven, waarbij de noodzaak en de gemaakte belangenafwegingen uitgebreider belicht zullen worden.

¹² URL: <http://www.kc-wetgeving.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/>

6. Functie FG

In het toetsmodel staat het volgende vermeld: *“Voor praktische en uitvoeringstechnische duiding van de vragen kunt u ook contact opnemen met de Functionaris Gegevensbescherming (FG), die binnen uw departement verantwoordelijk is voor het toezien op toepassing en naleving van de Wet bescherming persoonsgegevens. Als uw beleids- of wetgevingsvoorstel betrekking heeft op een ICT-project, neem dan ook tijdig contact op met uw departementale Chief Information Officer (CIO) die dit op strategisch niveau moet beoordelen.”*¹³

In het WRR-rapport *“iOverheid”* wordt geadviseerd om ook aandacht te besteden aan de intern toezichthoudende en adviserende taken van een FG.¹⁴ Bovengenoemd citaat gaat daar ten dele op in, maar geadviseerd wordt om nader uitwerking te geven aan de rol die de FG heeft als intern toezichthouder, onderscheidenlijk als intern adviseur.

7. Overige opmerkingen

Het CBP heeft nog gedetailleerde en redactionele opmerkingen (zie bijlage). Indien gewenst kan dit advies op ambtelijk niveau gedeeld worden.

Conclusie

Het CBP geeft u in overweging om de punten uit dit advies mee te nemen bij de uiteindelijke implementatie van het concept-toetsmodel.

¹³ Zie: concept-toetsmodel, p.2 (tweede bullit).

¹⁴ *Kamerstukken II* 2011-2012, 26 643, nr. 211, p. 7, 10 (Rapport *“iOverheid”* van de Wetenschappelijke Raad voor Regeringsbeleid d.d. 15 maart 2011).

Bijlage

Gedetailleerde opmerkingen

Hieronder zal het CBP paginagewijs en gedetailleerd ingaan op een aantal punten van het concept-toetsmodel.

Pagina 1:

Onder de zesde bullit wordt aangegeven dat de uiteindelijke beantwoording als basis en bron kunnen dienen voor de juridische verantwoording van beleidskeuzen in een Memorie van Toelichting. Dit kan echter ook een nota van toelichting zijn of zelfs toelichting bij ministeriële regeling of wellicht beleidsregel. Het CBP adviseert de minister om dit in het concept-toetsmodel aan te passen.

Onder de zevende bullit is aangegeven dat de "(...) PIA-beoordeling moet worden ondernomen door beleidsmedewerker/wetgevingsjurist van het ministerie/de uitvoeringsdienst/de (overheids-)instantie die "verantwoordelijke" is/zal zijn voor de verwerking van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens." Het kan echter zijn dat de daadwerkelijke verwerking niet plaatsvindt bij de overheidsinstantie dat het wetsvoorstel opstelt, maar bijvoorbeeld bij een uitvoeringsinstantie of provincie/gemeente. Hieruit volgt dat degene die de PIA invult niet altijd samenvalt met de verantwoordelijke voor de verwerking in de zin van artikel 1, onder d, Wbp. Het CBP adviseert de minister dit onderscheid nader te verduidelijken in het concept-toetsmodel.

Pagina 2:

Onder de eerste bullit staat vermeld dat het concept-toetsmodel onderdeel zal zijn van het IAK. Uit het concept-toetsmodel blijkt niet op welke manier de implementatie zal geschieden. Het CBP adviseert de minister om het IAK nader toe te lichten en/of in te leiden.

Onder het kopje "Wanneer" (derde alinea) staat: "Aangezien de noodzaak voor verwerking van persoonsgegevens als zodanig een belangrijke bouwsteen is voor de grondrechtelijke proportionaliteitstoetsing (...)" Het is echter andersom: de proportionaliteitstoetsing maakt (samen met de subsidiariteitstoetsing) onderdeel uit van het noodzakelijkheidsvereiste. Het CBP adviseert de minister om dit in het concept-toetsmodel aan te passen.

Pagina 5:

Onder vraag I.3 is de vraag of de persoonsgegevens "(...) beleidsmatig of technisch onontbeerlijk (...)" zijn en vervolgens wordt dat toegelicht met een verwijzing naar artikel 11 Wbp. Het CBP constateert dat op dit punt een aantal zaken door elkaar lopen. Er is de noodzakelijkheidseis (ofwel: onontbeerlijkheid) om gegevens te verwerken uit artikel 8 Wbp en vervolgens de relevantie-eis van artikel 11 Wbp. Het CBP adviseert in de eerste plaats om aan te sluiten bij de terminologie van de Wbp en geen onontbeerlijk te gebruiken maar noodzakelijkheid. In de tweede plaats adviseert het CBP om de toelichting op dit punt aan te passen.

Onder vraag I.5 staat vermeld: *“Loop het hele voorziene traject van persoonsgegevens na, en geef bij elk onderdeel aan om welk soort van de hiervoor genoemde verwerkingen het gaat.”* Het is onduidelijk wat de relevantie is van deze vraag. Maakt het uit of de verantwoordelijke bijvoorbeeld ordent of vastlegt? Het CBP adviseert de minister om nader toe te lichten waarom deze vraag is opgenomen.

Pagina 6:

Onder vraag II. 3 (toelichting) is artikel 9, lid 1, Wbp opgenomen. Het CBP adviseert om bij de toelichting over artikel 9 Wbp in elk geval de criteria op te nemen uit het tweede lid. In het tweede lid staan de criteria voor de onverenigbaarheidstoets.

Pagina 7:

Onder vraag II.4 wordt gesproken over *“de persoon die binnen de organisatie verantwoordelijk is voor kennisgeving.”* Wordt hier kennisgeving in de zin van informatieverstrekking als bedoeld in artikelen 33 en 34 van de Wbp bedoeld? Het CBP adviseert de minister om dit te verduidelijken.

Onder vraag II.4 is het onduidelijk waarom het gebruik van nieuwe persoonsgegevens voor een bestaand doel of het gebruik van bestaande gegevens voor een nieuw doel specifiek intern gecommuniceerd moeten worden bij persoon verantwoordelijk voor de kennisgeving en de FG en andere verwerkingen niet. Het is onduidelijk of hiermee de melding van verwerking van persoonsgegevens mee wordt bedoeld conform artikel 27 Wbp. Het CBP adviseert de minister om dit te verduidelijken en in elk geval het “melden” bij de FG (of indien niet aanwezig: het CBP) conform artikel 27 Wbp op te nemen in het concept-toetsmodel.

Vraag II.6 lijkt door de plek in het concept-toetsmodel alleen te zien op het gebruik van nieuwe persoonsgegevens voor een bestaand doel of het gebruik van bestaande gegevens voor een nieuw doel. De eis van artikel 11, tweede lid, Wbp geldt echter voor alle gegevensverwerkingen. Het CBP adviseert om deze vraag in een eerder onderdeel van het concept-toetsmodel op te nemen.

Onder vraag II.8 (toelichting) is artikel 42, lid 1, Wbp toegelicht. Het CBP adviseert om de criteria uit artikel 42, lid 2, Wbp ook op te nemen.

Pagina 8:

Zoals ook bij de algemene beoordeling is opgemerkt, is voor een aantal vragen onduidelijk wat de relevantie en/of gevolgen zijn van de beantwoording van de vraag. Bijvoorbeeld bij vraag III.5: *“(…) Omvat het register een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer) (…).”* Gelden er dan andere regels? Zo ja: welke? Dit wordt uit de toelichting niet duidelijk. Het CBP verzoekt – dit geldt overigens voor de meeste vragen uit het toetsmodel – om bij elke vraag de relevantie en gevolgen op te nemen.

Bij vraag III.6 (toelichting) staat vermeld: *“De Wbp (art. 76-77) bepaalt dat persoonsgegevens slechts naar een land buiten de EU (…).”* Echter, alleen artikel 76 Wbp bepaalt dat persoonsgegevens die aan een verwerking onderworpen zijn of die bestemd zijn om na hun doorgifte te worden

verwerkt slechts naar een land buiten de Europese Unie worden doorgegeven indien dat land een passend beschermingsniveau waarborgt. Artikel 77 geeft juist een aantal uitzonderingen op deze regel. Het CBP adviseert de minister om dit aan te passen.

In de toelichting bij vraag III.6 wordt ingegaan op de lijst van landen die volgens de Europese Commissie een passend niveau van gegevensbescherming waarborgen. Wat betreft de Verenigde Staten geldt dat de Europese Commissie heeft bepaald dat de organisaties die zich verplicht hebben tot naleving van de zogenoemde Safe Harbour Principles ook geacht worden een passend beschermingsniveau te waarborgen. Het CBP adviseert om in de toelichting bij vraag III.6 aan Safe Harbour aandacht te schenken.

Pagina 9:

Bij vraag IV. 5 wordt een vraag gesteld over de verwerking bij een bewerker. Het CBP verzoekt om hierbij ook het opstellen van een bewerkersovereenkomst te behandelen.

Bij vraag IV. 6 verzoekt het CBP om aan te sluiten bij de terminologie van de Wbp en derhalve op te nemen dat er technische en organisatorische beveiligingsmaatregelen zijn.

Onder vraag IV. 6 (toelichting) wordt voor het bepalen van het juiste risiconiveau verwezen naar de Achtergrondstudie 23 "Beveiliging van persoonsgegevens" (AV-23) van het CBP. Het CBP attendeert de minister erop dat deze AV-23 is vervangen door de 'Richtsnoeren Beveiliging van persoonsgegevens'.

Pagina 10:

Het CBP adviseert de minister om bij vraag V.2 te verduidelijken dat deze vraag voortvloeit uit artikel 33 Wbp. Dit geldt ook voor vraag V.3 dat uit artikel 34 Wbp voortvloeit.

Bij vraag V.4 wordt kort ingegaan op het begrip "toestemming." Het CBP adviseert om in het concept-toetsmodel ook aan de vereisten die bij toestemming spelen (vrij, specifiek, geïnformeerd) aandacht te besteden.

Pagina 11:

De toelichting van vraag V.6 lijkt niet te passen op de vraag zelf. Artikel 35, derde lid, ziet op derden die bezwaar kunnen hebben, en niet specifiek op andere organisaties die de gegevens hebben verzameld. Het CBP adviseert de minister om dit aan te passen.

Redactionele opmerkingen

- In de gehele tekst wordt de Wet bescherming persoonsgegevens afgekort met WBP. De juiste citeerwijze is: Wbp.
- Onder de tweede bullit van pagina 2 wordt IAK voor het eerst genoemd. Het CBP verzoekt om deze afkorting, omdat het voor het eerst wordt genoemd, voluit te schrijven: Integraal Afwegingskader voor Beleid en Regelgeving.

- Onder vraag I.1 van pagina 4 worden diverse definities (persoonsgegevens, verantwoordelijke en bewerker) genoemd. Het CBP verzoekt u om aan te sluiten bij de begripsbepalingen uit artikel 1 Wbp. Dit geldt overigens voor alle definities die genoemd worden in het gehele concept-toetsmodel.
- Onder vraag I.1 van pagina 4 worden de termen “verzameling” en “verwerking” naast elkaar genoemd, terwijl verzamelen een onderdeel vormt van de algemene Wbp-term “verwerking.” Het CBP verzoekt de Minister om de algemene term “verwerking” te hanteren in het concept-toetsmodel. Dit geldt voor het gehele concept-toetsmodel.
- Onder vraag II. 2 van pagina 6 wordt gesproken over “project” en onder vraag II.3 over “project/systeem.” Op pagina 1 staat vermeld dat de PIA een hulpmiddel is bij ontwikkeling van beleid en wetgeving. Het CBP adviseert om een eenduidige terminologie te hanteren en derhalve op deze plaats ook “ontwikkeling van beleid en wetgeving” te gebruiken.
- Onder vraag II. 3 (toelichting) van pagina 6 staat vermeld: “(...) of toevoeging van nadere persoonsgegevens voor het bereiken van een nader doel (..)” (onderstreping door het CBP toegevoegd). Het CBP neemt aan dat “nadere” vervangen dient te worden met “andere” en verzoekt de Minister om dit aan te passen.
- Onder vraag I.5 (toelichting) van pagina 5 staat de definitie van “verwerking” vermeld. Voor de volgordeadvies adviseert het CBP – gezien de relevantie - om deze definitie in de eerste vraag en/of stap van een PIA op te nemen.
- Onder vraag II.4 (toelichting) van pagina 7 moet artikel 43 veranderd worden in: artikel 62.
- Bij vraag IV.3 van pagina 9 wordt de term “gewist” gebruikt. Het CBP verzoekt de minister om in plaats van “wissen” aan te sluiten bij de Wbp-term “vernietigen.”
- Bij vraag V.1 van pagina 10 adviseert het CBP om de term ‘verwerken’ in plaats van ‘verzamelen’ gebruiken.