Evaluatie
Toetsmodel PIA Rijksdienst
Onderzoeksrapport

Uitgevoerd in opdracht van het ministerie van Binnenlandse zaken
en Koninkrijksrelaties.

Privacy Management Partners biedt praktische oplossingen voor behoorlijke
en zorgvuldige gegevensverwerking in overeenstemming met de wet.
www.pmpartners.nl

Evaluatie Toetsmodel PIA Rijksdienst

Onderzoeksrapport

auteurs
dr. J.A.G. (Koen) Versmissen CIPP/E
mr. drs. J.H.J. (Jeroen) Terstegge CIPP E/US
K.M. (Karen) Siemers LLM MA CIPP/E CIPM
T.H. (Wendy) Tran LLB CIPP/E CIPM

begeleidingscommissie van CZW BZK
mr. dr. P.M. (Pien) van den Eijnden
mr. drs. P.M. (Pauline) Verhaak

datum
20 mei 2016

Samenvatting

Het Toetsmodel PIA Rijksdienst dient vanaf 1 september 2013 standaard te worden toegepast bij het ontwikkelen van nieuwe wetgeving of beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien. Dit onderzoek ter evaluatie van het Toetsmodel brengt de concrete ervaringen van gebruikers met en hun waardering voor het Toetsmodel in kaart. Ook doet het op basis van de daaruit voortvloeiende inzichten concrete aanbevelingen voor de toekomst van het Toetsmodel. De evaluatie is uitgevoerd door middel van een literatuuronderzoek, interviews, een online enquête en een analyse.

De drie centrale onderzoeksvragen luidden:

1. Vervult het Toetsmodel een richtinggevende en corrigerende functie bij het gebruik van persoonsgegevens?
2. Sluit het Toetsmodel qua invulling en formulering aan bij de specifiek voor de overheid geldende vereisten om privacyaspecten te toetsen in een vroeg stadium van beleidsontwikkeling (in aanvulling op het bestaande instrumentarium om privacyaspecten van beleid- en wetgeving te toetsen)?
3. In hoeverre behoeft het Toetsmodel aanpassing in het licht van de vereisten die aan een PIA worden gesteld in artikel 35 van de komende Algemene Verordening Gegevensbescherming?

Richtinggevende en corrigerende functie

Heeft het Toetsmodel een daadwerkelijk positief effect op de behoorlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens? Dat blijkt inderdaad het geval te zijn, maar nog in vrij beperkte mate. Soms wordt een project stopgezet, vaker worden de verwerkingen van gegevens verbeterd of met meer waarborgen omkleed.
Het komt echter ook voor dat een PIA vooral als administratieve last wordt beschouwd, of dat aanbevelingen sneuvelen onder politieke of bestuurlijke druk. Inhoudelijke verbeteringen aan het Toetsmodel kunnen de effectiviteit ervan verbeteren; voor het goed uitvoeren van een PIA is privacydeskundigheid echter onontbeerlijk. Een bijkomend positief effect van het uitvoeren van een PIA is dat dit leidt tot een groter privacybewustzijn binnen de organisatie.

Invulling en formulering

Voldoet het Toetsmodel qua inhoud en qua proces? Qua inhoud blijkt er nog veel te verbeteren. Het gaat dan om zowel praktische toepasbaarheid, volledigheid, begrijpelijkheid, bruikbaarheid als gebruikersvriendelijkheid. De belangrijkste concrete verbeterpunten zijn het verminderen van juridisch taalgebruik, het scheiden van PIA's voor wetgeving en beleid en PIA's voor processen en systemen, en het ontwikkelen van een interactieve digitale versie van het Toetsmodel. Qua proces blijkt een belangrijk knelpunt het tijdig uitvoeren van de PIA. Debet hieraan is gebrek aan duidelijkheid over het proces; wanneer moet er bijvoorbeeld een PIA worden uitgevoerd, en wie moet daartoe opdracht geven? Meer in algemene zin lijdt het PIA-proces veelal onder een gebrek aan privacybewustzijn, privacydeskundigheid en verankering in de organisatie.

Algemene Verordening Gegevensbescherming

De PIA-benadering van het Toetsmodel blijkt zich goed te verhouden tot die van de AVG. Er zijn in die benadering dan ook geen fundamentele wijzigingen benodigd. Wel brengt de AVG verschillende aandachtspunten met zich mee voor de inhoud van een volgende versie van het Toetsmodel en voor het proces daaromheen.
Het betreft onder meer de vraag wanneer een PIA wel of niet verplicht is, verplichte onderdelen van een PIA en het consulteren van betrokkenen en de Functionaris voor de Gegevensbescherming. Uiteraard dient ook de vragenlijst van het Toetsmodel te worden aangepast aan de inhoudelijke wijzigingen in de AVG ten opzichte van de huidige regelgeving.

Op basis van bovenstaande conclusies en onze eigen expertise hebben we als belangrijkste aanbevelingen geformuleerd:

- Bevorder, om ervoor te zorgen dat PIA's op tijd en altijd wanneer het nodig is worden uitgevoerd, het privacybewustzijn binnen de Rijksoverheid.
- Bevorder, mede om ervoor te zorgen dat het privacybewustzijn binnen de Rijksoverheid toeneemt, het uitvoeren van PIA's.
- Maak onderscheid tussen enerzijds PIA's voor wetgeving of beleid, en anderzijds PIA's voor systemen of processen.
- Werk nader uit wat de criteria zijn wanneer al dan niet een PIA moet worden gedaan, en vertaal die naar een "PIA Quick Scan" die organisaties helpt om deze vraag te beantwoorden.
- Stel in plaats van een verplichte vragenlijst een verplicht kader op voor zowel de PIA zelf, de verslaglegging daarover als het PIA-proces, en vul dat aan met onder meer een model-vragenlijst, een model-opzet van een PIA-rapport en een model-PIA-proces.
- Ruim in het kader voldoende plaats in voor het beoordelen van de proportionaliteit van de voorgenomen gegevensverwerking.
- Ruim in het kader voldoende plaats in voor het in kaart brengen en beoordelen van de privacyrisico's, en voor het vaststellen van de maatregelen die zullen worden genomen om die risico's te vermijden of tot een acceptabel niveau terug te brengen.
- Verwerk het model-PIA-proces zoveel mogelijk in de model-vragenlijst, zodat uitvoerders als het ware vanzelf door het proces worden geleid.
- Maak het Toetsmodel gebruikersvriendelijker.

Lijst van afkortingen

AmvB	Algemene maatregel van Bestuur
AVG	Algemene Verordening Gegevensbescherming
BIR	Baseline Informatiebeveiliging Rijksdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
CIO	Chief Information Officer
CIP	Centrum voor Informatiebeveiliging en Privacybescherming
CZW	Directie Constitutionele Zaken en Wetgeving
DG	Directeur-Generaal
DPIA	Data Protection Impact Assessment
DWJZ-WKB	Directie Wetgeving en Juridische Zaken, Afdeling Wetgevingskwaliteitsbeleid
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris voor de Gegevensbescherming
IAK	Integraal Afwegings Kader voor Beleid en Regelgeving
ICO	Information Commissioner's Office
MvT	Memorie van Toelichting
NEN/ISO	Nederlands Normalisatie-instituut/ Internationale Organisatie voor Standaardisatie
PIA	Privacy Impact Assessment
PIAF	Privacy Impact Assessment Framework
VenJ	Ministerie van Veiligheid en Justitie
Wbp	Wet bescherming persoonsgegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Afkortingen in Bijlage I

ALT	Alternatief model
TPR	Toetsmodel PIA Rijksdienst

Inhoudsopgave

Inleiding

In mei 2011 neemt de Eerste Kamer de motie Franken c.s. aan. Deze verzoekt de regering om voorstellen voor nieuwe wetgeving waarbij sprake is van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer te toetsen op, onder meer, “de resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico’s de maatregel met zich meebrengt”[1].

Vanaf 1 september 2013 moet het Toetsmodel PIA Rijksdienst standaard worden toegepast bij het ontwikkelen van nieuwe wetgeving of beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien.
Uit correspondentie van het kabinet met de Tweede Kamer blijkt dat het Toetsmodel nog niet altijd even consequent wordt toegepast en dat er bij nieuwe wetgeving nog niet altijd op een inzichtelijke manier verslag wordt gedaan van de resultaten van het Toetsmodel. In de kabinetsvisie op privacy is in mei 2015 gerefereerd aan het Toetsmodel als één van de toetsstenen bepalend voor het privacybeleid.

Bij de aanbieding van het Toetsmodel is toegezegd dat het gebruik ervan binnen twee jaar na inwerkingtreding zal worden geëvalueerd. Dit document is het eindrapport van het onderzoek ter evaluatie van het Toetsmodel. Het onderzoek is uitgevoerd door Privacy Management Partners in opdracht van de directie Constitutionele Zaken en Wetgeving van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Het eerstvolgende hoofdstuk geeft een introductie over het Toetsmodel.
Daarna formuleren we in hoofdstuk 2 de doel- en vraagstelling van het onderzoek en beschrijven we onze aanpak. Op basis van de uitkomsten van het literatuuronderzoek, de interviews en de enquête beantwoorden we eerst de deelvragen, en daarna de centrale onderzoeksvragen in hoofdstuk 3 en 4. De conclusies van het onderzoek geven ons tot slot aanleiding tot het doen van een aantal concrete aanbevelingen in hoofdstuk 5. De eerste drie bijlagen van het rapport betreffen gedetailleerde rapportages van de drie onderzoeksfasen. Ze worden gevolgd door het Toetsmodel zoals dit in 2013 door de minister voor Wonen en Rijksdienst, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Veiligheid en Justitie, aan de Tweede Kamer is gestuurd.[2] In de laatste bijlage is een lijst met geïnterviewden personen opgenomen en noemen we de begeleidingscommissie van dit onderzoek.

1. Kamerstukken I 2010/11, 31 051, D (motie Franken c.s.), p. 1.
2. Kamerstukken II 2012/13, 26 643, nr. 282 en bijlage.

1 Over het Toetsmodel PIA Rijksdienst

1.1 Inhoud

Het Toetsmodel PIA Rijksdienst wordt sinds 1 september 2013 verplicht toegepast bij ontwikkeling van nieuwe wetgeving en systemen die zien op de verwerking van persoonsgegevens.[3] Hiermee wordt invulling en uitvoering gegeven aan de motie-Franken, het regeerakkoord "Bruggen Slaan" en maatregelen die in de iStrategie van de Rijksoverheid zijn aangekondigd ter versterking van de aandacht voor privacy bij grote ICT-projecten.[4]

Een Privacy Impact Assessment (PIA) is een hulpmiddel om de privacyrisico's van (voorgenomen) gegevensverwerkingen op een gestructureerde en heldere wijze in kaart te brengen. Het Toetsmodel is specifiek gericht op de Rijksdienst en bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen.

Het Toetsmodel bestaat uit één document dat in twee vormen in omloop is. Het officiële Toetsmodel bestaat uit een toelichtende inleiding, gevolgd door een lijst van feitelijke en technische vragen, gebaseerd op nationale en Europese privacyvereisten (zie bijlage IV). Bij elke vraag is een toelichting geschreven bestaande uit definities, verwijzingen naar de wet of voorbeelden. In de praktijk wordt soms ook gewerkt met een uitgeklede versie van het Toetsmodel. Deze onofficiële versie van het Toetsmodel is een Word-document met alle vragen, maar zonder de inleiding of de toelichtingen per vraag.

Daarnaast is er nog de "PIA Light". Deze verkorte versie van het Toetsmodel is geen apart document, maar wordt in het Toetsmodel als volgt omschreven:

---

3. "Het is niet nodig om de gehele vragenlijst af te werken als het gaat om:
   - uitbreiding van het databestand binnen een bestaand ICT-systeem (volstaan kan worden met beantwoording van de vragen in secties I en IV)
   - gebruik van een bestaand databestand of ICT-systeem voor aanvullende of nieuwe doelen (volstaan kan worden met beantwoording van de vragen in sectie II en IV)
   - koppeling van verschillende al bestaande databestanden of ICT-systemen voor bestaande of aanvullende of nieuwe doelen (volstaan kan worden met beantwoording van de vragen in secties II-V)

   Vanzelfsprekend is het bij het uitvoeren van een dergelijke "PIA-light" verstandig terug te grijpen op eventuele eerdere stukken (uitgevoerde PIA's, andere impact assessments, toelichtingen)."[5]

Om tot slot verwarring te voorkomen, duiden we ook de term PIA Quick Scan of privacy quick scan. Hiermee wordt doorgaans een test bedoeld waarmee kan worden vastgesteld of het nodig is dat er een PIA wordt uitgevoerd. Deze test wordt in de literatuur aangeduid als 'threshold analysis (initial assessment)'[6] of 'screening questions'[7]. Op dit moment is een dergelijke Quick Scan niet officieel door de overheid ter beschikking gesteld als instrument.

1.2 Doelstellingen Toetsmodel PIA Rijksdienst

In de visie van het kabinet vormt het, waar nodig, uitvoeren van een PIA één van de acht centrale toetsstenen van privacybescherming.[8] Het kabinet verwijst daarbij expliciet naar het Toetsmodel. Het Toetsmodel is zowel richtinggevend als corrigerend bedoeld en daarmee geen vrijblijvende exercitie.[9] Het heeft daarmee een sturend

karakter en is niet bedoeld als een juridische compliancetoets. In een reactie op vragen van de Kamercommissie VenJ in 2013 over het Toetsmodel wordt aangegeven dat juridische normen zijn vertaald naar feitelijke vragen die in het beginstadium van beleidsvorming kunnen spelen of andere informatie kan achterhalen die noodzakelijk is voor wel afgewogen besluitvorming. De antwoorden dienen als input voor de overige meer juridisch getinte toetsingsinstrumenten.[10] De regering heeft aangegeven dat het Toetsmodel is bedoeld als een aanvulling op reeds bestaande toetsinstrumenten.[11] Het Toetsmodel stelt de risicobenadering (al dan niet theoretisch) centraal in de toelichting, terwijl bij een juridische compliancetoets de nadruk ligt op het voldoen aan concrete normen uit de Wbp.[12]

In de toelichting bij het Toetsmodel staat wat er met de resultaten van een ingevulde vragenlijst dient te gebeuren. Deze dienen in ieder geval te worden toegezonden aan de betrokken Functionaris voor de Gegevensbescherming (FG) en Chief Information Officer (CIO). Vervolgens hangt het af van de context hoe de resultaten verder moeten worden verwerkt. Bij het beleid dat de bouw van ICT-systemen of de aanleg van databestanden voorziet is dat anders dan bij wetgeving. In de eerstgenoemde situatie zal de FG volgens de toelichting advies kunnen geven bij het bepalen van de nodige maatregelen en waarborgen. CIO's zullen de resultaten gebruiken voor advisering over informatiebeveiliging en systeemontwerp. Daarnaast kunnen de resultaten van een systeem-PIA worden gebruikt voor het melden bij de Autoriteit Persoonsgegevens (AP) of de FG. Voor PIA's op wetgeving geldt dat een samenvatting van de belangrijkste afwegingen en keuzes moet worden opgenomen in de Memorie van Toelichting. Daarvoor geeft de toelichting van het Toetsmodel ook een modelpassage die hiervoor kan worden gebruikt:

> "Gezien de aard van dit voorstel is in de fase van beleidsontwikkeling een Privacy Impact Assessment uitgevoerd (zie ook Kamerstukken I 2010/11, 31051, nr. D; motie-Franken). Met behulp hiervan is de noodzaak van gegevensverwerking bekeken, en 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 de betrokkenen. [Beschrijving specifieke aspecten en de in dit geval gemaakte belangenafweging]"[13]

3. Aanbiedingsbrief Toetsmodel PIA-Rijksdienst van de Minister voor Wonen en Rijksdienst, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie, 21 juni 2013.
4. Eerste Kamer, vergaderjaar 2010–2011, 31 051, D; Bruggen Slaan – Regeerakkoord VVD-PvdA, 29 oktober 2012, p. 28; Kamerstukken II, 2011–2012, 26643, nr. 216, p. 10.
5. Toetsmodel PIA Rijksdienst, p. 3.
6. EU PIAF Project, "Recommendations for a privacy impact assessment framework for the European Union". Deliverable D3, november 2012, p. 24–25.
7. UK Informations Commissioner's Office, "Conducting privacy impact assessments code of practice", februari 2014, p. 20–21.
8. Kamerstukken II, 2014–2015, 32761, nr. 83 (visie op privacy).
9. Toetsmodel PIA Rijksdienst, p. 1.
10. Kamerstukken I, 2013–2014, 31051 G.
11. Zoals binnen de Rijksoverheid de Leidraad afstemming wetgeving op de Wbp. Zie Kamerstukken II 2014/15, 26 643 nr. 335 (reactie op motie Segers/Oosenbrug).
12. De Autoriteit Persoonsgegevens had ook sterk afgeraden om de PIA als compliancetoets vorm te geven. Zie College Bescherming Persoonsgegevens, brief aan Ministerie van BZK over het concept Toetsmodel Privacy Impact Assessment, 5 maart 2013.
13. Toetsmodel PIA Rijksdienst, p. 4.

2 Doelstellingen evaluatie

2.1 Onderzoeksvragen

Dit onderzoek beoogt de concrete ervaringen van gebruikers met en hun waardering voor het Toetsmodel in kaart te brengen. De evaluatie is opgezet om zowel positieve ervaringen als ondervonden knelpunten aan het licht te brengen. Daartoe zijn door de opdrachtgever de onderstaande drie centrale onderzoeksvragen geformuleerd.

1. Vervult het Toetsmodel een richtinggevende en corrigerende functie bij het gebruik van persoonsgegevens?
2. Sluit het Toetsmodel qua invulling en formulering aan bij de specifiek voor de overheid geldende vereisten om privacyaspecten te toetsen in een vroeg stadium van beleidsontwikkeling (in aanvulling op het bestaande instrumentarium om privacyaspecten van beleid- en wetgeving te toetsen)?
3. In hoeverre behoeft het Toetsmodel aanpassing in het licht van de vereisten die aan een PIA worden gesteld in artikel 35 van de komende Algemene Verordening Gegevensbescherming?

De eerste centrale onderzoeksvraag hebben wij geïnterpreteerd als gericht op het daadwerkelijke positieve effect dat het toepassen van het Toetsmodel heeft op de behoorlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens.
De tweede vraag hebben wij opgevat als betrekking hebbend op zowel de inhoud van het Toetsmodel als het daarin beschreven proces van uitvoering ervan.

De centrale onderzoeksvragen zijn door de opdrachtgever uitgewerkt tot een aantal concrete deelvragen, onderverdeeld in drie categorieën: Wanneer, Hoe, Resultaat. De drie categorieën zien op specifieke aspecten van het Toetsmodel. Ze dienen ter ondersteuning van de twee eerste centrale onderzoeksvragen.

Wanneer

- Hoeveel PIA's zijn er bij het Rijk verricht sinds de invoering van het Toetsmodel (uitgesplitst naar de categorieën wetgeving, beleid en uitvoering)?
- In welke gevallen wordt een PIA gedaan (en in welke gevallen niet)?
- In welke fase van de besluitvorming wordt een PIA toegepast?
- In welke gevallen bestaat er behoefte aan een "PIA light" of een "privacy quick scan" (in de toelichting op het toetsmodel staat dat kan worden volstaan met het beantwoorden van enkele vragen als het gaat om wijziging van regels of een praktijk van bestaande gegevensuitwisseling)?
- Hoe kan nader worden verduidelijkt in welke gevallen het Toetsmodel PIA rijksdienst moet worden toegepast (en wanneer niet)?

Hoe

- Hoe ervaren de gebruikers de bruikbaarheid van het Toetsmodel? Gebruikers zijn: opdrachtgevers en uitvoerders van de PIA, geïnterviewden, personen of organisaties die de resultaten moeten beoordelen en personen of organisaties die de resultaten moeten laten meewegen in hun uiteindelijke beslissing.
- Weten ambtenaren wanneer er een PIA moeten worden gedaan en hoe zij dat moeten (laten) aanpakken?
- Wordt een PIA intern verricht of extern uitbesteed?
- Wie is verantwoordelijk voor de uitvoering van een PIA?
- Hoeveel capaciteit is beschikbaar voor een PIA en hoe wordt deze bepaald?

- Is de rolverdeling helder (tussen beleidsambtenaren, wetgevingsjuristen, functionarissen voor de gegevensbescherming (FG), Chief information officer (CIO))?
- Is de vragenlijst begrijpelijk en volledig? Is deze toegesneden op de praktijk?
- Wordt het Toetsmodel PIA Rijksdienst gebruikt, of (ook) andere modellen?

Resultaat

- Hoe wordt verslag gedaan van de uitkomsten van een PIA?
- Met wie worden de uitkomsten van een PIA gedeeld (denk aan FG en CIO)?
- Hoe beschouwen externe organisaties de resultaten van een PIA op basis van hun expertise en rol (denk aan de Autoriteit Persoonsgegevens, maatschappelijke belangenorganisaties)?
- Op welke wijze wordt het resultaat van een PIA betrokken in de uiteindelijke besluitvorming? Wat is de rol of status van een PIA-rapportage daarbij?

De antwoorden op de deelvragen komen aan de orde in de eerste paragrafen in het volgende hoofdstuk, die op de bijbehorende centrale onderzoeksvragen de laatste twee paragrafen in het volgende hoofdstuk. De onderzoeksvraag over de Algemene Verordening Gegevensbescherming wordt beantwoord in hoofdstuk 4.

2.2 Aanpak

De evaluatie hebben wij in vier fasen uitgevoerd: een literatuuronderzoek, interviews, een enquête en een analyse. In de eerste onderzoeksfase hebben wij aan de hand van hoofdzakelijk openbare bronnen de doelstellingen van, opvattingen over, ervaringen met en waardering voor het Toetsmodel verkend. Daarnaast hebben wij op basis van enkele “best practice” documenten relevante elementen van en aandachtspunten voor PIA’s in kaart gebracht en deze toegepast op het Toetsmodel. Ook hebben we in kaart gebracht welke eisen de Algemene Verordening Gegevensbescherming aan PIA’s gaat stellen.

Vervolgens hebben wij op basis van het literatuuronderzoek en de onderzoeksvragen een interviewschema opgesteld. Op basis van dit schema hebben wij door middel van een selecte steekproef een gemêleerd gezelschap systematisch gevraagd naar ervaringen met het Toetsmodel. In totaal hebben wij dertig interviews gehouden met inhoudelijke en ervaringsdeskundigen. In de samenstelling van geïnterviewden zijn in ieder geval vertegenwoordigd de verschillende functies van FG, CIO en DG tot beleidsmedewerker, wetgevingsjurist en privacyspecialist werkzaam binnen de overheid. Daarnaast hebben we ook een aantal onafhankelijke experts gesproken vanuit diverse achtergronden. De interviews gaven toegang tot ervaringen met en opvattingen over PIA’s in het algemeen en het Toetsmodel in het bijzonder, gebaseerd op zowel algemene privacydeskundigheid als praktijkervaring. Mede door de diversiteit van de geïnterviewden is de input van de interviews met name een basis voor de kwalitatieve analyse.

In de derde fase van het onderzoek hebben we door middel van een online enquête een aantal vergelijkbare vragen uitgezet bij een specifieke doelgroep, te weten: niet reeds geïnterviewde personen die werkzaam zijn bij de Rijksoverheid en concrete ervaring hebben opgedaan met het Toetsmodel. Dit hebben wij gedaan door naar een aantal geselecteerde emailadressen de link naar de online enquête verzenden. Daarnaast hebben we de link verspreid via het Rijksportaal en een besloten forum[14] voor informatiebeveiliging- en privacyprofessionals bij de overheid. Personen die niet in de specifieke doelgroep vielen werden na een aantal selectievragen uit de enquête geleid. Zo konden respondenten die, geen concrete ervaring hebben opgedaan met het Toetsmodel, in principe ook geen specifieke vragen over het Toetsmodel beantwoorden. Ruim 50 personen binnen de doelgroep hebben zo kunnen bijdragen aan het onderzoek. Het doel van deze enquête was onder meer het toetsen en kwantificeren van de uitkomsten van de interviewfase.

Op basis van de hierboven beschreven fasen hebben wij een ruime hoeveelheid kennis en inzichten verworven, die ons in staat stelden om de drie centrale onderzoeksvragen en de bijbehorende deelvragen te beantwoorden en op basis daarvan conclusies te trekken ter evaluatie van het Toetsmodel. Daarnaast hebben wij vervolgens enkele aanbevelingen gedaan ter verbetering van het Toetsmodel.

14. CIP-pleio.nl

3 Het Toetsmodel in de praktijk

In dit hoofdstuk gaan we in op de in het vorige hoofdstuk opgesomde onderzoeksvragen. Eerst behandelen we de deelvragen in de eerste drie paragrafen 3.1. Daarbij volgen we de daar gehanteerde indeling op drie aspecten, te weten: het wanneer, het hoe en het resultaat van het gebruik van het Toetsmodel. Vervolgens komen we in de laatste twee paragrafen op basis van het literatuuronderzoek, de interviews, de enquête, onze analyse tot beantwoording van de eerste twee centrale onderzoeksvragen.

3.1 Wanneer

Hoeveel PIA's zijn er bij het Rijk verricht sinds de invoering van het Toetsmodel (uitgesplitst naar de categorieën wetgeving, beleid en uitvoering)?

Deze vraag is lastig concreet te beantwoorden. We hebben tijdens de interviews geprobeerd inzicht te krijgen in de kwantiteit van PIA's in de praktijk. Daarbij bleek dat de meeste geïnterviewden weinig zicht hadden op het aantal uitgevoerde PIA's bij hun organisatie, al waren er wat dat betreft wel duidelijke verschillen tussen organisaties. Er is geen centrale registratie van PIA's. Verschillende geïnterviewden gaven aan dat zij graag een dergelijk overzicht zouden bewerkstelligen. Op basis van de informatie die ons hierover tijdens het onderzoek ter ore is gekomen, schatten we in dat er sinds 1 september 2013 ten minste enkele honderden PIA's zijn uitgevoerd bij de Rijksoverheid. Het is niet uitgesloten dat het werkelijke aantal hiervan een veelvoud bedraagt. Hierbij maken we de kanttekening dat het aantal niets zegt over het aantal situaties waarbij geen PIA is gedaan terwijl dat eigenlijk wel had gemoeten.

Wij hebben aan zowel geïnterviewden als respondenten in de enquête gevraagd bij hoeveel PIA's ze betrokken zijn geweest. Daarbij hebben we een onderscheid gemaakt tussen PIA's op wetgeving, PIA's op beleid, en PIA's op processen of systemen. In die inventarisatie kwamen PIA's op wetgeving het meest voor en ook PIA's op beleid waren goed vertegenwoordigd. PIA's op systemen werden minder vaak genoemd. Uit interviews kwam als mogelijke verklaring voor het lagere aantal systeem-PIA's naar voren dat systemen vaak al voor de invoering van het Toetsmodel zijn opgezet en (al dan niet) getoetst. Ook werd genoemd de vermoedelijke onbekendheid met het feit dat bij het koppelen, aanpassen of anders gaan gebruiken van bestaande systemen eveneens een PIA moet worden uitgevoerd. Dat dit minder speelt als het gaat om beleid of wetgeving kan te maken hebben met het voorgeschreven Integraal Afwegingskader voor Beleid en Regelgeving (IAK), dat de uitvoerder stapsgewijs langs het Toetsmodel leidt. Een andere reden die is genoemd voor het verschil in aantallen, is dat het Toetsmodel zich beter leent voor wetgevings- en beleids-PIA's dan voor systeem-PIA's.

Overigens lag het aantal PIA's waarbij de geïnterviewden betrokken zijn geweest ver uiteen. Daarbij is de rol van de geïnterviewden én het departement waar zij werkzaam zijn van grote invloed. De hoeveelheid bij FG's varieerde van 5 tot 30 PIA's en bij de personen in uitvoerende rol tussen de 1 en 5 PIA's. Bij de enquête lag het aantal beduidend lager: daar gaf een meerderheid aan bij één of twee PIA's betrokken te zijn geweest. De respondenten met een klein aantal PIA's hebben dan ook in de meeste gevallen aangegeven in de uitvoerende rol betrokken zijn geweest bij een PIA.

In welke gevallen wordt een PIA gedaan (en in welke gevallen niet)?

Op concreet en kwantitatief niveau is niet goed aan te geven wanneer wel en geen PIA is gedaan. Dit vloeit deels voort uit het hierboven geconstateerde gebrek aan overzicht van uitgevoerde PIA's. Een bepalende factor voor het wel uitvoeren van PIA's blijkt te zijn of er personen zijn die daar actief op aansturen. Het is echter lastig om uitspraken

te doen over wanneer er geen PIA's worden gedaan, zeker wanneer dat eigenlijk wel zou moeten. Zelfs Functionarissen voor de Gegevensbescherming (FG's) geven aan daar in het algemeen geen inzicht in te hebben, en vaak pas van een eventuele PIA-verplichting op de hoogte raken doordat de PIA is uitgevoerd en zij het resultaat krijgen toegezonden.

In welke fase van de besluitvorming wordt een PIA toegepast?
Dit blijkt heel divers te zijn: soms wordt een PIA uitgevoerd voorafgaand aan of in de voorfase van een traject, soms tijdens de rit, en soms pas tegen het einde of een enkele keer zelfs na afloop.

Een PIA uitvoeren tegen het einde of na afloop van een traject, blijkt geen goed idee te zijn. In zowel de interviews als de enquête werd aangekaart dat PIA's dan vaak worden toegeschreven naar bepaalde keuzes of maatregelen. De PIA heeft dan nauwelijks meer een corrigerende functie. Beslissingen zijn veelal reeds genomen, waardoor bijvoorbeeld wordt beoordeeld of een gegevenswerking op de minst ingrijpende manier plaatsvindt (subsidiariteit), maar niet of de verwerking überhaupt in verhouding staat tot het doel dat ermee gediend wordt (proportionaliteit). Dit beeld wordt ook herkend door de Autoriteit Persoonsgegevens (AP). Een suggestie die in dit verband werd gedaan was het concreet aangeven van de nadelen van het te laat ontdekken van of aandacht geven aan privacyissues, zoals extra geld en tijd die het kost om zaken in een laat stadium alsnog in orde te maken.

Wanneer PIA's eerder worden uitgevoerd, worden ze over het algemeen als nuttig ervaren. Zowel geïnterviewden als respondenten geven aan dat een PIA het best zo vroeg mogelijk in een traject kan worden uitgevoerd, al erkennen sommigen daarbij dat dit op dit moment nog een streven is. Een PIA in een zo vroeg mogelijk stadium uitvoeren maakt het mogelijk om met open vizier na te denken over de risico's en om nog zonder grote nadelige consequenties privacybestendige keuzes te maken.

In welke gevallen bestaat er behoefte aan een "PIA light" of een "privacy quick scan"?[15]
Het Toetsmodel geeft aan dat het in drie gevallen niet nodig is om de gehele vragenlijst af te werken. Dit feit blijkt echter door lang niet alle geïnterviewden te zijn opgemerkt. Ook bij de enquête gaven verscheidene respondenten aan deze "PIA light" niet te kennen of nooit te hebben gebruikt. Sommige geïnterviewden gaven aan de PIA light te hebben toegepast in de daarvoor bedoelde gevallen. Enkelen gaven zelfs aan dat ze de PIA light ook zouden willen toepassen op beleidsvoornemens, wetsaanpassingen en op voorheen vrijgestelde systemen. Het argument hiervoor waren met name de snelheid en efficiëntie van de verkorte versie. Anderzijds waren er ook geïnterviewden die een PIA-light resoluut afwezen omdat in hun ogen alleen een volledige PIA de mogelijkheid biedt om goed en diep na te denken over voorgenomen gegevensverwerkingen.
Deze opvatting zagen we ook terug in de enquête. Daarin gaf ruim de helft van de respondenten overigens aan het eens te zijn met de stelling dat de light versie van het Toetsmodel een zinvolle uitbreiding is.

Sommige geïnterviewden gebruikten de termen "PIA-light" of "privacy quick scan" om een (andere) behoefte te uiten. Deze bestaat uit een korte test die alleen tot doel heeft om te beoordelen of er een PIA moet worden gedaan. Hierbij werd enkele malen verwezen naar het criterium 'likely high risk' uit de Algemene Verordening Gegevensbescherming (AVG).

Hoe kan nader worden verduidelijkt in welke gevallen het Toetsmodel PIA Rijksdienst moet worden toegepast (en wanneer niet)?
Deze vraag is in feite op twee manieren beantwoord. De vraag gaat over handvatten om vast te stellen of voor een bepaald traject al dan niet een PIA uitgevoerd moet worden. Dat blijkt echter al snel te leiden tot beschouwingen over bewustwording: om de vraag "wel of geen PIA?" te kunnen beantwoorden, moet die immers eerst gesteld worden.

Waar het gaat om de genoemde handvatten wordt de bij de vorige vraag toegelichte "privacy quick scan" gezien als een goed instrument om te verhelderen wanneer een PIA gedaan moet worden.

Waar het gaat om bewustwording is de verwachting bij velen dat dit zich deels vanzelf oplost door het verstrijken van de tijd. De ruim twee jaar die ten tijde van de interviews waren verstreken sinds de invoering van het Toetsmodel vormden volgens diverse geïnterviewden een relatief korte tijd, waardoor een en ander nog moest landen. Wel zou volgens de meerderheid zeker bij personen die slechts incidenteel met een PIA te maken krijgen het idee moeten worden bevorderd dat het Toetsmodel geen checklist is, maar veel meer een hulpmiddel. Een andere gedane suggestie is dat het Toetsmodel dwingender voorgeschreven dient te worden, bijvoorbeeld door zonder PIA geen volgende fase in te kunnen met een project. Zo noemt een respondent de huidige PIA-verplichting slechts op papier verplicht.

3.2 Hoe

Hoe ervaren de gebruikers de bruikbaarheid van het Toetsmodel?[16]

Gebruikers zijn verdeeld over de bruikbaarheid van het Toetsmodel. We zien hier overigens een discrepantie tussen de interviews en de enquête. In alle gevallen zijn de positieve en negatieve antwoorden redelijk in balans. In de interviews wordt echter op alle vragen op dit terrein licht negatief gescoord,[17] terwijl in de enquête bij één vraag de positieve en negatieve antwoorden gelijk op gaan en bij de overige vragen licht positief wordt gescoord. Het gaat dan over begrijpelijkheid, volledigheid, bruikbaarheid en gebruikersvriendelijkheid.

Een ander veel benoemd knelpunt, zowel in de interviews als in de enquête, is het juridische taalgebruik in het Toetsmodel. Dit blijkt vaak te leiden tot onduidelijkheid of een verkeerd begrip bij de personen die de vragenlijst invullen. Verschillende FG's gaven aan dat zij in de praktijk geregeld antwoorden tegenkomen met een heel andere insteek dan bedoeld in de vraag.

De aanbevelingen op dit punt gaan twee verschillende kanten op. Sommigen geven aan dat het taalgebruik gemakkelijker moet, zonder juridisch jargon. Anderen zijn van mening dat het onderliggende probleem, de complexiteit en open normen van het privacyrecht, daarmee niet wordt weggenomen. Hun suggestie is om bij het uitvoeren van een PIA volgens het Toetsmodel een privacydeskundige te betrekken.

Waar het gaat over de volledigheid van de vragenlijst van het Toetsmodel geven sommigen aan dat zij de lijst te uitgebreid vinden, terwijl anderen juist belangrijke onderdelen missen of onvoldoende aanwezig achten. In dat laatste verband zijn de volgende onderwerpen genoemd:

- een beschrijving van de verwerking zelf, als startpunt van de PIA;
- het volledig in kaart brengen van het nut en de noodzaak van de gegevensverwerking;
- toetsing op proportionaliteit;
- toetsing van de grondslag voor elke verwerking;
- vragen over (sub)bewerkers;
- een goede risico-inschatting;
- concrete handvatten voor een eigenaar van een verwerking.

Weten ambtenaren wanneer er een PIA moeten worden gedaan en hoe zij dat moeten (laten) aanpakken?

De stelling dat het duidelijk is wanneer er een PIA moet worden uitgevoerd wordt licht positief beantwoord. Het Toetsmodel biedt hier dus kennelijk wel de nodige houvast, maar er is zeker nog ruimte voor verbetering. Dat merken we ook uit de resultaten van de enquête. Daar gaf een grote meerderheid aan dat PIA's soms niet worden uitgevoerd omdat degene die daar verantwoordelijk voor is niet weet van de PIA-verplichting. Hetzelfde beeld zien we als het gaat om de aanpak in de praktijk. Bij de interviews

wordt de stelling dat het PIA-proces in de praktijk goed loopt gemiddeld beoordeeld met ‘enigszins mee eens’. Bij de enquête beoordeelt een kleine meerderheid deze stelling met (enigszins tot) niet mee eens.

Verklaringen voor de gegeven positieve antwoorden zijn gerelateerd aan verwijzingen naar het IAK of naar stimulerende personen bij het departement of de afdeling waar de persoon werkzaam is. Voor de antwoorden die aangeven dat het niet duidelijk is, geldt dat soms wordt aangegeven dat er geen privacy officer is die daar op toe ziet. Daarnaast noemt men ook dat er soms problemen ontstaan doordat het te laat duidelijk wordt dat er een PIA gedaan moet worden.

Wordt een PIA intern verricht of extern uitbesteed?
PIA’s worden voor het merendeel geheel of grotendeels intern verricht. Een belangrijk argument hiervoor is de bijdrage die dit levert aan het privacybewustzijn van de betrokken medewerkers. Daarbij komen de nadelen van het inhuren van externe partijen: naast de kosten is tevens genoemd de diversiteit in resultaten die daarvan het gevolg kan zijn. De noodzaak van het betrekken van privacydeskundigen bij het uitvoeren van een PIA wordt breed onderschreven. In dat verband gaf een respondent aan dat het inschakelen van externe privacydeskundigheid belangrijke meerwaarde had bij de eerste paar keer dat de betreffende organisatie een PIA uitvoerde.

Wie is verantwoordelijk voor de uitvoering van een PIA?
Deze vraag kan op verschillende manieren worden begrepen, namelijk als verwijzend naar het opdrachtgeverschap van de PIA of naar de feitelijke uitvoering ervan. In de interviews hebben we gevraagd naar het opdrachtgeverschap van PIA’s. Dat blijkt in de praktijk nogal divers te zijn, min of meer gelijk verdeeld over de eerste lijn—denk hierbij bijvoorbeeld aan de verantwoordelijke directeur of de projectleider—en de tweede lijn—zoals de FG, de (wetgevings)jurist of de CIO.

Hoeveel capaciteit is beschikbaar voor een PIA en hoe wordt deze bepaald?
In de interviews hebben wij gevraagd naar het aantal uur dat gemiddeld aan een PIA wordt besteed. Over het algemeen is aangegeven dat dit altijd zal afhangen van de grootte en complexiteit van de gegevensverwerking. Bij kleine projecten kon het soms in één dag, terwijl er ook projecten zijn genoemd waaraan alles bij elkaar wel meer dan honderd manuren zijn besteed. Een andere factor vormen ook de ‘leeruren’ die personen nodig hebben wanneer zij voor het eerst een PIA uitvoeren.

Is de rolverdeling helder tussen beleidsambtenaren, wetgevingsjuristen, Functionarissen voor de Gegevensbescherming (FG), Chief information officer (CIO)?
De stelling dat de rolverdeling tussen de bij de PIA betrokken personen helder is, wordt door de meeste geïnterviewden beantwoord met ‘enigszins mee eens’. Het Toetsmodel biedt hier dus kennelijk de nodige houvast, maar er is een grote mate van diversiteit tussen de personen onderling. Twee van de geïnterviewden scoorden zeer negatief terwijl er ook twee juist zeer positief scoorden. Dit is te verklaren door de situatie dat op sommige departementen grote verschillen zijn in begeleiding. Is er veel gedaan om het proces te doen verbeteren, dan is de rolverdeling helder. Dit komt volgens deze personen niet door (de toelichting bij) het Toetsmodel maar door eigen beleid. Anderen geven juist aan dat in het Toetsmodel helder genoeg staat wie wat moet doen. Deze beoordeling wijkt af van die van de respondenten in de enquête. Van hen vond 60% dat de rolverdeling niet of niet helemaal helder is. Vanuit deze groep is expliciet aangegeven dat het hen zou helpen als de rolverdeling helderder zou worden beschreven.

Specifiek ten aanzien van de rol van de FG blijkt dat die per departement significant kan verschillen. Bij sommige departementen is heel duidelijk welke rol de FG heeft in het PIA-proces. Andere keren is die onduidelijk, op twee mogelijke manieren: ofwel de FG is niet pro-actief aanwezig, ofwel de uitvoerders van de PIA hebben het (onjuiste)

idee dat de FG niet een toezichthouder is maar meer een adviseur op het gebied van de Wbp.[18] Onduidelijkheid over de rol van de FG lijkt er mede debet aan dat niet altijd helder is wie er met de uitkomsten van een PIA aan de slag moet.

Wordt het Toetsmodel PIA Rijksdienst gebruikt, of (ook) andere modellen?
Hoewel het Toetsmodel is voorgeschreven, worden er ongeveer net zo vaak alternatieve instrumenten ingezet. Het gaat dan om de PIA-instrumenten van de Belastingdienst, NOREA of SURF, of om zelf opgestelde modellen. Als reden voor de keuze voor alternatieve instrumenten wordt vooral de ervaring genoemd dat gebruik van het Toetsmodel tot te veel onduidelijkheid leidt. Dat maakt dat degenen die de vragenlijst zelf invullen te vaak bij anderen om hulp moeten vragen. Ook de ervaren onvolledigheid van het Toetsmodel is voor sommigen aanleiding om naar een alternatief instrument te grijpen.

Soms worden de alternatieve instrumenten ingezet in plaats van het Toetsmodel, soms ook in aanvulling daarop. Enkele respondenten geven aan het Toetsmodel als “verplicht nummer” te beschouwen,[19] in aanvulling waarop zij dan gebruik maken van het alternatieve instrument dat hun voorkeur heeft.

3.3 Resultaat

Hoe wordt verslag gedaan van de uitkomsten van een PIA?
In ongeveer een derde van de gevallen blijft de rapportage over de PIA beperkt tot de ingevulde vragenlijst. In de overige gevallen werd een volledige PIA-rapportage opgeleverd, of werden de uitkomsten van de PIA verwerkt in bijvoorbeeld een beleids- of projectdocument.

Een aantal kernelementen van het resultaat van een PIA zijn: een beschrijving van systemen en processen, een beschrijving van de verwerkte persoonsgegevens, een juridische analyse, een overzicht van de privacyrisico’s, een overzicht van de informatiebeveiligingsrisico’s en aanbevelingen voor het voorkomen of mitigeren van de onderkende risico’s. Vrijwel al deze onderdelen blijken over het algemeen minimaal op beperkte wijze in PIA-rapportages aan de orde te komen. In de interviews komt naar voren dat rapportages op basis van alternatieve PIA-instrumenten net iets vaker deze elementen niet beperkt, maar ruimschoots bevatten. Juridische analyses zijn zo goed als altijd aanwezig. Een discrepantie die we slechts marginaal kunnen verklaren zien we als het gaat om aanbevelingen voor het voorkomen en het mitigeren van risico’s. Waar we uit de interviews afleiden dat die niet of beperkt aanwezig zijn, levert de enquête op dit punt een positievere score op (beperkt of ruimschoots). Hierbij kan een rol spelen dat een aantal van de geïnterviewden ofwel in de rol als FG, ofwel in de rol als privacydeskundige kritischer zijn op het eindresultaat van de PIA-rapportage. In de groep respondenten zien we een substantieel deel aan de uitvoerderskant in plaats van in een beoordelende of toezichthoudende rol.

Buiten het verband van deze specifieke vraag is enkele malen aangegeven dat PIA-rapportages nog wel eens onvolledig willen zijn. De verklaring hiervoor wordt dan gezocht in het feit dat sommige vragen in het Toetsmodel waarschijnlijk te lastig te begrijpen waren voor degene die de PIA heeft uitgevoerd. Volgens een aantal geïnterviewden ontbreken uiteindelijk vaak drie essentiële aspecten: een goede risico-inschatting, het volledig in kaart brengen van het nut en de noodzaak van de gegevensverwerking en een proportionaliteitstoets. Door de personen die de PIA uitvoeren wordt dan ook aangegeven, dat ze het lastig vinden om risico’s te benoemen.

Met wie worden de uitkomsten van een PIA gedeeld (denk aan FG en CIO)?
De uitkomst van een op basis van het Toetsmodel uitgevoerde PIA dient te worden toegezonden aan de FG en de CIO. In driekwart van de PIA’s blijken de resultaten te worden toegezonden aan de FG, in de helft ook aan de CIO. In enkele gevallen worden de resultaten ook aan anderen gezonden, met name aan de bij de PIA betrokken partijen (in de brede zin), aan de Autoriteit Persoonsgegevens[20] en aan het parlement.

In de enquête hebben wij de respondenten gevraagd met wie naar hun mening de definitieve PIA-resultaten gedeeld zouden moeten worden. Er blijkt een duidelijke voorkeur te bestaan voor openheid over de uitkomsten van een PIA. De grootste groep zou de definitieve resultaten willen delen met het (project)team, het MT, de politieke leiding en andere betrokken departementen c.q. Rijksdiensten. De groep respondenten die daarna het grootste is zou de resultaten zelfs openbaar willen maken. Wel wordt erop gewezen dat in dat geval onopgeloste (technische of beveiligings-)problemen van openbaarmaking uitgezonderd zouden moeten worden. Genoemde argumenten voor openheid over de uitkomsten van PIA's zijn het verspreiden van inzichten in risico's, zorgen dat de verantwoordelijkheid bij de juiste personen komt te liggen en brede kennisdeling in de organisatie.

Hoe beschouwen externe organisaties de resultaten van een PIA op basis van hun expertise en rol?

Om zicht te krijgen op het antwoord op deze vraag hebben wij gesproken met vertegenwoordigers van de volgende externe organisaties:

- de Autoriteit Persoonsgegevens
- een maatschappelijke belangenorganisatie (Privacy First)
- de Raad van State
- het College voor de Rechten van de Mens

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) schetst het beeld dat met het Toetsmodel alleen dan een zuivere belangenafweging kan plaatsvinden (en daarmee een meerwaarde gerealiseerd) indien het in het voortraject of aan het begin van een project wordt toegepast. In die fase van het proces of project is er nog ruimte om eventuele aandachtspunten uit een PIA te betrekken omdat er nog ruimte is voor het maken van keuzes of het formuleren van uitgangspunten. Daarbij is een belangrijke randvoorwaarde dat het PIA-instrument met de juiste kennis en ervaring wordt toegepast. Kennis maakt de uitkomst van een PIA, aldus de AP. Het Toetsmodel is daarbij echter niet meer dan een hulpmiddel en geen doel op zich. Het belangrijkste is dat op het juiste moment op de juiste wijze de belangen worden afgewogen. Daarbij speelt behalve kennis over de uitleg en toepassing van de Wbp, ook de beschikbaarheid van die kennis een rol. De AP heeft de indruk dat niet bij alle ministeries de beschikbaarheid van deze kennis dezelfde aandacht krijgt. In 2014 heeft de toezichthouder een kort onderzoek gedaan naar de PIA's bij wetgevingsadviezen. Daaruit kwam naar voren dat overal waar de AP een PIA verwachtte, deze ook was uitgevoerd (tussen de 15 en 20 stuks in 2014). Het feit dat er een PIA was voltooid had evenwel geen direct aantoonbaar verband met een positiever advies van de AP over het wetsvoorstel. Het AP heeft dit niet verder geanalyseerd maar heeft de indruk dat met name bij de noodzakelijkheidstoets er voorbeelden zijn waar naar een doel wordt toe geredeneerd in plaats van een gemotiveerde afweging van belangen in het kader van noodzaak, proportionaliteit en subsidiariteit. De betrokkenheid van FG's lijkt volgens de AP groter bij de systeem-PIA's dan bij wetgeving-PIA's, maar verschilt per ministerie.

Maatschappelijke belangenorganisatie

In het interview met Privacy First is aangegeven dat zij nog geen PIA-rapportages hebben kunnen gebruiken bij het bespreken of ter discussie stellen van privacyissues. Dat had ook te maken met het feit dat veel van deze issues al dateren van voor de invoering van het Toetsmodel. Privacy First gaf aan dat het geheel aan procedurele elementen in een PIA de onafhankelijkheid van de uitvoerder ervan moet borgen. Indien een ministerie zelf de PIA uitvoert op een project waarbij allerlei belangen meespelen, heeft dit de schijn van een slager die zijn eigen vlees keurt. Inhoudelijk verwacht Privacy First dat er voldoende aandacht komt voor een strikte toetsing afgeleid vanuit artikel 8 EVRM. Vanuit dit perspectief noemt de organisatie vier hoofdcriteria waaraan een PIA dient te voldoen: onafhankelijkheid, objectiviteit, strikte toetsing aan noodzaak en de proportionaliteits- en subsidiariteitstoets.
Het consulteren van stakeholders in de zin van maatschappelijke organisaties is een kans voor de overheid om kritiek kenbaar te maken maar ook het maatschappelijk

draagvlak aan te voelen. Dit raakt de opvatting dat PIA's altijd openbaar toegankelijk zouden moeten zijn, iets dat volgens de belangenorganisatie haaks staat op de huidige werkelijkheid. Tot slot werd opgemerkt dat de resultaten bij wetgeving deels in de Memorie van Toelichting dienen te worden opgenomen. Privacy First ziet veel waarde in de mogelijkheid om het volledige rapport te kunnen raadplegen. Op die manier kan, indien nodig, aanvullende informatie over de PIA waar slechts kort naar wordt gerefereerd in de Memorie van Toelichting worden opgezocht.

Raad van State
De resultaten van PIA's bereiken niet altijd de Raad van State. Daarover ontstaat wel eens discussie met partijen, dat verschilt per ministerie. Inhoudelijk ontbreekt soms de toets op proportionaliteit, of is de doelbinding niet volledig uitgewerkt. Soms ontstaat er wel eens overlap met de wetgevingsadviestaak van de AP. De Raad ziet zijn taak echter meer in het kader van brede advisering, en is niet in dezelfde mate als de AP gespecialiseerd in privacy en de Wbp. PIA's kunnen helpen om een en ander ook voor de Raad van State inzichtelijk te maken. In PIA-rapportages ziet de Raad graag meer aanknopingspunten voor beantwoording van de proportionaliteitsvraag.
Daarnaast vindt de Raad het een gemis dat informatie uit de PIA-rapportage anders dan de conclusies doorgaans niet terugkomt in de Memorie van Toelichting. Denk aan het noemen van de alternatieve manieren van gegevensverwerking waarvoor (bewust) niet is gekozen. Dat soort informatie kan de Parlementaire Geschiedenis completer maken en hulp bieden in juridische geschillen.

College voor de Rechten van de Mens
Bij het College voor de Rechten van de Mens was het Toetsmodel als zodanig nog niet bekend. Wel kijkt het College ook naar privacyaspecten in wetgevingsadviezen, zoals bij de Wet op de inlichtingen- en veiligheidsdiensten. In de Memorie van Toelichting van dit conceptwetsvoorstel stonden een aantal overwegingen op privacygebied waarvan het College nadrukkelijk vraagt om verdere onderbouwing. Van het delen (en beoordelen) van volledige PIA-rapporten is niet of nauwelijks sprake. Dit heeft met name te maken met de specifieke technische deskundigheid inzake gegevensverwerkingen die bij het College schaars is. Aangegeven wordt dat het College wel kritisch kan adviseren, maar toch altijd een buitenstaander blijft als het gaat om de procesinrichting. Privacyadviezen van het College gaan bijvoorbeeld over het feit dat proportionaliteit beoordeeld dient te worden aan de hand van bestaande jurisprudentie in plaats van de praktijk. Op dat abstractere niveau ziet het College wel mogelijkheden om sporadisch als een gesprekspartner op te treden.

Op welke wijze wordt het resultaat van een PIA betrokken in de uiteindelijke besluitvorming? Wat is de rol of status van een PIA-rapportage daarbij?
Deze vraag hebben wij ruimer geïnterpreteerd. In de interviews hebben we gevraagd naar de daadwerkelijke effecten die het uitvoeren van een PIA sorteert. Het uitvoeren van een PIA blijkt veelal een behoorlijk positief effect te hebben. Dit geldt het sterkst voor het zicht krijgen op privacyrisico's en het komen tot een zorgvuldigere omgang met persoonsgegevens, en in iets mindere mate voor de corrigerende of richtinggevende functie van de PIA. Uit een vergelijking tussen de beoordeling van effecten door middel van het Toetsmodel en door middel van een alternatief PIA-instrument blijkt dat voor bijna alle effecten geldt dat het Toetsmodel positiever scoort.

In de enquête konden respondenten aangeven welke effecten de toepassing van het Toetsmodel feitelijk teweeg heeft gebracht én welke effecten zij zelf wensen voor het Toetsmodel. Het verschil bleek niet heel groot. Het eerste antwoord op beide vragen was een groter privacybewustzijn in de organisatie. De tweede plaatsen weken wel af. Feitelijk is het tweede grootste huidige effect meer inzicht in de details van de verwerkingen van persoonsgegevens, terwijl dat volgens de respondenten bij voorkeur meer inzicht in de privacyrisico's zou moeten zijn.

3.4 Richtinggevende, corrigerende functie van het Toetsmodel

De eerste centrale onderzoeksvraag luidt als volgt:
Vervult het Toetsmodel een richtinggevende en corrigerende functie bij het gebruik van persoonsgegevens?

Wij hebben deze vraag opgevat als betrekking hebbend op het daadwerkelijke positieve effect dat het toepassen van het Toetsmodel heeft op de behoorlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens. Daarvoor is niet alleen nodig dat privacyaspecten in de PIA op de juiste manier aan de orde komen, maar ook dat de conclusies en aanbevelingen van de PIA daadwerkelijk en adequaat opgepakt worden.

In de toelichting bij het Toetsmodel is aangegeven dat het richtinggevende en corrigerende karakter ervan tot uiting komt in de vragen, die uitnodigen tot het formuleren van antwoorden of, wanneer dit reeds is gebeurd, tot het opnieuw beoordelen van de antwoorden tijdens het invullen van het Toetsmodel. Tot op zekere hoogte blijkt dit in de praktijk inderdaad zo te werken. Hoewel er nog volop ruimte is voor verbetering van de inhoud van het Toetsmodel,[21] blijkt dat toepassing ervan desondanks vaak wel degelijk daadwerkelijke positieve effecten heeft. Tegelijkertijd moet geconstateerd worden dat die effecten vrij beperkt lijken te zijn, zodat ook op dat vlak nog stappen te zetten zijn.

In enkele gevallen (waarbij het PIA's betrof op wetgeving) werden de onderliggende ontwikkelingen geheel of gedeeltelijk stopgezet dan wel significant inhoudelijk gewijzigd. Vaker bleef de essentie van het onderliggende project behouden (niet zelden vanwege wensen vanuit de politiek), maar werden er verbeteringen doorgevoerd in de gegevensverwerking of de waarborgen voor de rechtmatigheid, behoorlijkheid en zorgvuldigheid daarvan, zowel rechtstreeks (aanpassingen aan voorgenomen verwerkingen) als via wijzigingen in het wetsvoorstel. Ook heeft de PIA geholpen om aspecten van gegevensverwerking te onderbouwen, bijvoorbeeld in een Memorie van Toelichting. Het uitvoeren van PIA's heeft niet alleen (in sommige gevallen) een direct positief effect op de verwerking van persoonsgegevens, maar levert vaak ook een belangrijke bijdrage aan toename van het privacybewustzijn van de bij de PIA betrokken medewerkers. In die zin is er dus ook nog sprake van een niet te onderschatten indirect positief effect.

Inhoudelijke verbeteringen aan het Toetsmodel zijn waar het de kwaliteit van de PIA-rapportage betreft slechts een deel van het antwoord. Privacy en de bescherming van persoonsgegevens blijven nu eenmaal complexe materie met veel open normen. Het is mogelijk om een nieuwe versie van het Toetsmodel op te stellen met veel aandacht voor de eisen en wensen van de verschillende soorten gebruikers. Maar ook dan zal gelden dat voor het goed uitvoeren van een PIA privacydeskundigheid onontbeerlijk is. Die deskundigheid zal dus (intern of extern) voorhanden en in te zetten moeten zijn.

Een gedegen PIA-rapportage heeft niet zonder meer ook invloed op de besluitvorming. In een aantal gevallen is die invloed er wel degelijk. Daartegenover staan de gevallen waarin het uitvoeren van een PIA vooral gezien wordt als een administratieve last (het invullen van een afvinklijst). Soms heeft dat te maken met tekortschietend privacybewustzijn in een organisatie, waardoor de PIA te laat in het proces wordt uitgevoerd of gezien wordt als een juridische compliancetoets. Maar soms zit het probleem ook dieper, en is er sprake van politieke druk om bepaalde verwerkingen van persoonsgegevens hoe dan ook door te laten gaan en op een al vastgestelde manier vorm te geven. Dat heeft uiteraard een sterke negatieve impact op het corrigerende karakter van de PIA.

Resumerend stellen wij vast dat toepassing van het Toetsmodel weliswaar tot de beoogde daadwerkelijke positieve effecten leidt, maar niet in alle gevallen, en ook niet altijd in dezelfde mate.

3.5 Inhoud en proces Toetsmodel

De tweede centrale onderzoeksvraag luidt als volgt:
Sluit het Toetsmodel qua invulling en formulering aan bij de specifiek voor de overheid geldende vereisten om privacyaspecten te toetsen in een vroeg stadium van beleidsontwikkeling (in aanvulling op het bestaande instrumentarium om privacyaspecten van beleid- en wetgeving te toetsen)?

Wij hebben deze vraag opgevat als betrekking hebbend op zowel de inhoud van het Toetsmodel als het daarin beschreven proces van uitvoering ervan. Op beide gaan we hieronder achtereenvolgens nader in.

3.5.1 Inhoud

Op verschillende aspecten met betrekking tot de inhoud van het Toetsmodel valt er nog veel te verbeteren. Het gaat dan om zowel praktische toepasbaarheid, volledigheid, begrijpelijkheid, bruikbaarheid als gebruikersvriendelijkheid.

Voor verschillende situaties en doelgroepen is het Toetsmodel te juridisch van aard, en daarmee moeilijk hanteerbaar. Dat leidt in de praktijk tot frustratie bij de pogingen om de vragen goed te beantwoorden. Alternatieve PIA-instrumenten, zoals het NOREA-model, scoren in dit opzicht beter met minder juridische taalgebruik (zonder dat de verwijzingen naar de wetgeving ontbreken).

Het Toetsmodel is in zijn huidige vorm bedoeld voor zowel PIA's voor wetgeving of beleid als voor PIA's voor systemen. Met betrekking tot laatstgenoemde geven zowel geïnterviewden als respondenten aan dat het Toetsmodel daarvoor minder geschikt is dan voor PIA's op wetgeving of beleid. Dat heeft in sommige gevallen te maken met de technische (en niet juridische) achtergrond van ICT-personeel dat wel te maken krijgt met de juridisch ingestoken vragen. Het is zeer de vraag of het mogelijk is om beide toetsen werkelijk in één instrument te vangen: beleids- of wetgevings-PIA's vergen namelijk een meer abstracte toets op de fundamentele rechten en vrijheden zoals gewaarborgd door het EVRM en het Handvest van de Grondrechten van de EU, terwijl bij PIA's voor processen en systemen de focus ligt op concretere eisen die zijn terug te voeren op de Wbp en andere privacywetgeving.

Gebruikersvriendelijkheid zit hem behalve in de inhoud ook in de vorm.
Het Toetsmodel wordt in zijn huidige vorm ervaren als onoverzichtelijk en erg tekstueel ingestoken. In navolging van het gebruik van een alternatief PIA-instrument, het SURF-model, is door zowel geïnterviewden als respondenten geopperd om een digitale versie van de vragenlijst te maken. Specifieker werd als groot voordeel van het SURF-model genoemd het overzicht in één oogopslag van risico's en te nemen beveiligingsmaatregelen. Een doordachte digitale variant van het Toetsmodel die via de browser in te vullen is, zou aan dit bezwaar in belangrijke mate tegemoet kunnen komen.

3.5.2 Proces

Bij het ontwikkelen van het Toetsmodel is gekozen voor vragen die de juridische normen vertalen naar feitelijke vragen die in het beginstadium van beleidsvorming vaak spelen of behulpzaam zijn bij het achterhalen van andere informatie die noodzakelijk is voor welafgewogen besluitvorming. Het idee is, met andere woorden, dat een PIA vroeg in een traject wordt uitgevoerd, opdat deze daadwerkelijk invloed kan hebben op de invulling ervan. In de praktijk blijkt het door verschillende oorzaken niet altijd zo te gaan.

Veel van die oorzaken zijn terug te voeren op een gebrek aan duidelijkheid.
Er ontbreken voldoende duidelijke criteria voor wanneer er een PIA uitgevoerd moet worden. Voor zover wel helder is dat een PIA noodzakelijk is, is vervolgens de vraag aan de orde wie er dan voor verantwoordelijk is dat de PIA ook daadwerkelijk uitgevoerd gaat worden. Dit blijkt onvoldoende duidelijk, waardoor in de praktijk het

uitvoeren van een PIA geregeld niet wordt opgepakt omdat niemand zich daarvoor verantwoordelijk voelt. PIA's blijken in de praktijk ook allerlei verschillende soorten opdrachtgevers te hebben. Onduidelijkheid over opdrachtgeverschap is overigens slechts ten dele met behulp van het Toetsmodel op te lossen, aangezien verschillende organisaties hun relevante processen en verantwoordelijkheden op verschillende manieren hebben vormgegeven.

Een heel andere oorzaak waardoor het toetsen in een vroeg stadium soms niet wordt gehaald is dat niet altijd voldoende duidelijk is dat de verplichting tot het uitvoeren van de PIA ook betekent dat de uitkomsten van de PIA moeten worden betrokken in de besluitvorming. Dat is wel het geval, gelet op met name de Wbp en de in de Algemene wet bestuursrecht verankerde beginselen van behoorlijk bestuur.

Meer in algemene zin lijdt het PIA-proces onder een gebrek aan privacybewustzijn en privacydeskundigheid. Dat heeft als gevolg dat de vragen uit het Toetsmodel geregeld met te weinig diepgang, op niet relevante wijze of zelfs onjuist beantwoord worden. Dat komt een corrigerende of richtinggevende functie niet ten goede. De positieve keerzijde van deze medaille is dat het uitvoeren van een PIA een significante bijdrage levert aan het vergroten van het privacybewustzijn bij de betrokken medewerkers. Workshops waarin ook een privacydeskundige vertegenwoordigd is blijken effectief voor het delen van kennis én om meters te maken in het PIA-proces. Voor sommige organisaties is dit effect een belangrijke overweging om een PIA zoveel mogelijk zelf uit te voeren in plaats van er externe adviseurs bij te betrekken.

Een terugkerend thema in de interviews is ook dat de effectiviteit van het uitvoeren van een PIA sterk samenhangt met de verankering van het PIA-proces in de organisatie. De aanwezigheid van, zoals een van de geïnterviewden het omschreef, een "ecosysteem op privacygebied" blijkt een zeer positieve invloed te hebben op zowel de kwantiteit als de kwaliteit van de uitgevoerde PIA's.

15. In de toelichting op het Toetsmodel staat dat kan worden volstaan met het beantwoorden van enkele vragen als het gaat om wijziging van regels of een praktijk van bestaande gegevensuitwisseling. Zie paragraaf 1.1 van dit rapport.
16. Gebruikers zijn: opdrachtgevers en uitvoerders van de PIA, geïnterviewden, personen of organisaties die de resultaten moeten beoordelen en personen of organisaties die de resultaten moeten laten meewegen in hun uiteindelijke beslissing.
17. De antwoorden in de interviews waren zelfs negatiever als het gaat over de toepasbaarheid van het Toetsmodel in de praktijk. Deze laatste beoordeling was het meest negatief bij PIA's uitgevoerd door uitvoeringsinstanties en bij systeem-PIA's. Dit hangt vermoedelijk samen met het veel genoemde punt dat het Toetsmodel in zijn huidige vorm beter geschikt is voor PIA's voor wetgeving of beleid dan voor PIA's voor systemen.
18. Wat hier mee kan spelen is door enkele FG's is aangestipt: zowel departementen als FG's zelf blijken soms verschillende opvattingen te hebben over wat de rol van een FG inhoudt. Sommige FG's gaan alleen over interne aangelegenheden van het departement, andere hebben ook een rol gekregen of opgepakt ten aanzien van het beleidsterrein.
19. Niet iedereen is zich daar overigens van bewust. Eén respondent gaf aan dat het fijn zou zijn als het Toetsmodel zou worden voorgeschreven als instrument, omdat er nu te veel PIA-instrumenten zijn om uit te kiezen.
20. In het kader van een (al dan niet wettelijk verplichte) adviesaanvraag.
21. Zie daarvoor de volgende onderzoeksvraag.

4 De Algemene Verordening Gegevensbescherming

In dit hoofdstuk zullen wij de laatste hoofdvraag beantwoorden. Dit doen we door eerst in paragraaf 4.1 te kijken naar welke vereisten de AVG stelt aan een PIA. In paragraaf 4.2 leggen we die vereisten naast het huidige Toetsmodel en beantwoorden we de vraag in hoeverre het Toetsmodel aanpassing behoeft om eraan te voldoen.

4.1 Vereisten uit de AVG

Artikel 35 van de Algemene Verordening Gegevensbescherming[22] bepaalt dat een Data Protection Impact Assessment (DPIA)[23] moet worden uitgevoerd als het waarschijnlijk is dat het type verwerking of het gebruik van nieuwe technologie, gelet op de aard, reikwijdte, context en doeleinden van de verwerking, resulteert in een hoog risico voor de rechten en vrijheden van de mensen.[24] De AVG wijst daarbij een drietal gevallen aan waarin in ieder geval een DPIA moet worden uitgevoerd:

- een systematische en extensieve evaluatie van persoonlijke aspecten van mensen, die is gebaseerd op een geautomatiseerde verwerking, waaronder begrepen profiling, en waarop besluiten worden gebaseerd die juridisch effect sorteren jegens de betrokkene of hem in aanmerkelijke mate raken;
- grootschalige verwerking van bijzondere gegevens dan wel grootschalige verwerkingen van data met betrekking tot strafrechtelijke veroordelingen en overtredingen, en grootschalige verwerkingen van biometrische gegevens;
- grootschalige en systematische monitoring van voor het publiek toegankelijke plaatsen.

Deze lijst kan worden aangevuld door de toezichthouder, voor Nederland de Autoriteit Persoonsgegevens. Voorts kan de toezichthouder een lijst vaststellen met verwerkingen waarvoor juist geen DPIA hoeft te worden uitgevoerd. Daarnaast is een DPIA niet verplicht als de verwerking voortvloeit uit Unierecht dan wel uit nationale wetgeving, tenzij de Lidstaat het nodig vindt dat daarvoor wel een DPIA wordt uitgevoerd (art. 35 lid 10). Onduidelijk is of deze bepaling de bevoegdheid voor de Lidstaten inhoudt om hiervoor regels te stellen en dus alle (dan wel bepaalde categorieën) verwerkingen die uit de wet voortvloeien aan een DPIA te onderwerpen, of dat het slechts om een ad hoc keuze per verwerking/project gaat.

Een belangrijk aanknopingspunt voor de toepassing van artikel 35 is het woord ‘waarschijnlijk’ (likely). Dit impliceert dat aan het uitvoeren van de DPIA een proces voorafgaat om vast te stellen of een voorgenomen verwerking in aanmerking komt voor een DPIA. Dit proces ontbreekt momenteel in het Toetsmodel. Hoewel vragen 2a t/m 2e een aanzet zijn voor een dergelijke check,[25] leidt een ontkennend antwoord op ieder van die vragen nu niet tot de conclusie dat er geen PIA hoeft te worden uitgevoerd.

Het Toetsmodel PIA Rijksdienst hinkt momenteel op twee gedachten, namelijk het vaststellen van risico’s voortvloeiend uit wetgeving of beleid én het vaststellen van risico’s in voorgenomen overheidsverwerkingen. Daardoor heeft het Toetsmodel dus een breder toepassingsbereik dan strikt genomen wordt voorgeschreven door artikel 35 AVG, dat—gelet op de voorschriften over de inhoud van een DPIA in het zevende lid—lijkt te slaan op de tweede groep (systemen, processen) en niet de eerste groep (wetgeving/beleid).

Daar komt bij dat artikel 36 AVG voor wetsvoorstellen, die de verwerking van persoonsgegevens met zich brengen, juist niet voorschrijft dat er een DPIA op wordt uitgevoerd, maar slechts dat de toezichthouder over het wetsvoorstel wordt geconsulteerd. Dat laat overigens onverlet dat de AVG er niet aan in de weg lijkt te staan dat wetsvoorstellen wel worden onderworpen aan een DPIA om zo ook de dialoog met de toezichthouder te bevorderen.

Artikel 35 lid 7 AVG stelt ook eisen aan de inhoud van de DPIA. Die dient in ieder geval te bevatten:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan.

Momenteel worden PIA's nog op twee verschillende manieren vormgegeven. Een PIA kan een adviserend karakter hebben, over de conclusies en met name aanbevelingen waarvan de verantwoordelijke nog een besluit dient te nemen, of de PIA kan een weergave omvatten van de maatregelen waartoe gelet op de onderkende risico's feitelijk besloten is. Onder de AVG wordt, gelet op het laatste van deze inhoudelijke eisen, het laatste type PIA de norm.

Artikel 35 lid 9 AVG schrijft voor dat consultatie van betrokkenen of hun vertegenwoordigers, waar mogelijk, onderdeel moet zijn van de DPIA. Ook dit ontbreekt momenteel in de toelichting in deel A van het Toetsmodel. Bovendien blijkt dat uitvoerders van PIA's die stakeholders bij het proces proberen te betrekken, soms grote moeite hebben om betrokkenen of organisaties die hen vertegenwoordigen te raadplegen. Hoewel het grootste deel van de respondenten aangaf aan deze verplichting te kunnen voldoen en ook weten welke organisaties ze kunnen benaderen, is een bijna even groot deel er niet van overtuigd dat hen dat lukt. Een niet veel kleiner deel van de respondenten vinden consultatie onwenselijk. Hiervoor zijn als argumenten aangegeven de werkbaarheid, tijd, het praktisch organiseren, het niet kunnen voldoen aan verwachtingen die bij de geconsulteerden kunnen ontstaan, en het risico op (bewuste) vertraging en belemmering door vertegenwoordigende organisaties.

Wanneer er een FG is aangewezen, dient ook die op grond van artikel 35 lid 2 AVG verplicht geconsulteerd te worden bij de uitvoering van de DPIA. Deze bepaling zal bij gebruik van het Toetsmodel vrijwel altijd van toepassing zijn, aangezien artikel 37 lid 1 onder a AVG overheidsinstanties verplicht tot het aanwijzen van een FG.

Artikel 35 lid 11 AVG, ten slotte, bepaalt dat de verantwoordelijke de DPIA dient te actualiseren in geval van wijzigingen in (de risico's die gepaard gaan met) de verwerking. Ook dit ontbreekt momenteel in de toelichting in deel A van het Toetsmodel.

Naast de procedurele bepalingen in artikel 35 AVG zijn uiteraard ook relevant de inhoudelijke wijzigingen in privacynormen in de AVG in vergelijking met de huidige regelgeving (Richtlijn 95/46 en de Wbp). De vragenlijst van het Toetsmodel zal daarop moeten worden aangepast.

4.2 Vereisten Algemene Verordening Gegevensbescherming

De derde centrale onderzoeksvraag luidt als volgt:
In hoeverre behoeft het Toetsmodel aanpassing in het licht van de vereisten die aan een PIA worden gesteld in artikel 35 van de komende Algemene Verordening Gegevensbescherming?

Uit de analyse in de vorige paragraaf blijkt dat de benadering van het Toetsmodel zich goed verhoudt tot die van de AVG. Er zijn in die benadering dan ook geen fundamentele wijzigingen benodigd. Wel brengt de AVG de onderstaande aandachtspunten met zich mee voor de inhoud van een volgende versie van het Toetsmodel en het proces eromheen.

- Het Toetsmodel dient rekening te houden met, of ten minste te verwijzen naar, hetgeen de Autoriteit Persoonsgegevens heeft bepaald over situaties waarin een DPIA wel of niet verplicht is.
- Het Toetsmodel dient de verantwoordelijke te helpen bij het beantwoorden van de vraag of het uitvoeren van een DPIA verplicht is.
- De verplichte elementen van een DPIA, te weten: beschrijving verwerking, beoordeling noodzaak en proportionaliteit, beoordeling risico's en beoogde risicobeperkende maatregelen dienen in het Toetsmodel een duidelijke plaats te krijgen.
- Het Toetsmodel dient duidelijk te maken dat, indien mogelijk, betrokkenen geconsulteerd moeten worden. Gelet op de moeite die dit veel organisaties blijkt te kosten, is een handreiking hiervoor op zijn plaats.
- Het Toetsmodel dient duidelijk te maken dat de FG moet worden geconsulteerd.
- Het Toetsmodel dient duidelijk te maken dat de PIA moet worden geactualiseerd als zich significante wijzigingen voordoen in de verwerking of de risico's die ermee gepaard gaan.
- De vragenlijst van het Toetsmodel dient te worden aangepast aan de inhoudelijke wijzigingen in de AVG ten opzichte van de huidige regelgeving.

22. De AVG-artikelnummers verwijzen naar de definitieve versie zoals gepubliceerd op 6 april 2016.
23. De Nederlandse vertaling spreekt van een 'Gegevensbeschermingseffectbeoordeling'.
24. Voor de volledigheid merken we op dat artikel 35 onder invloed van de onderhandelingen tussen het Europees Parlement en de Raad is gewijzigd ten opzichte van de het ontwerp van de Europese Commissie. Waar het ontwerp sprak over 'specific risks' spreekt het onderhandelingsresultaat over 'high risks'. Daarmee wordt de lat voor het uitvoeren van DPIA's hoger gelegd dan in het ontwerp.
25. Vergelijk ook het lijstje met risicofactoren in de Beleidsregels Meldplicht Datalekken (p. 26/27) om vast te stellen of sprake is van een 'ernstig datalek' dat moet worden gemeld bij de toezichthouder.

5 Conclusies en aanbevelingen

Na het beantwoorden van de onderzoeksvragen zoomen we in dit hoofdstuk uit en kijken we terug op onze bevindingen. Aan de inzichten die dat oplevert, koppelen we concrete aanbevelingen voor de toekomst van het Toetsmodel. Die zijn gebaseerd op de uitkomsten van het onderzoek, aangevuld met onze eigen expertise. We beginnen met enkele algemene conclusies en aanbevelingen, en gaan daarna dieper in op achtereenvolgens de inhoud en vorm van het Toetsmodel en het proces eromheen.

5.1 Algemeen

Er is een wisselwerking tussen privacybewustzijn en PIA's. In organisaties waar sprake is van een hoge mate van privacybewustzijn worden meer en betere PIA's uitgevoerd, en hebben de uitkomsten daarvan meer invloed op de voorgenomen verwerking van persoonsgegevens. Omgekeerd kan PIA's uitvoeren en de uitkomsten daarvan serieus nemen een belangrijke bijdrage leveren aan het, mede in het licht van de AVG, zo noodzakelijke privacybewustzijn in alle lagen van een organisatie. Voorwaarde voor dat laatste is wel dat er voldoende interne betrokkenheid is bij de PIA.

Aanbevelingen

- Bevorder, om ervoor te zorgen dat PIA's op tijd en altijd wanneer het nodig is worden uitgevoerd, het privacybewustzijn binnen de Rijksoverheid.
- Bevorder, mede om ervoor te zorgen dat het privacybewustzijn binnen de Rijksoverheid toeneemt, het uitvoeren van PIA's. In het bijzonder:
  - Stel het uitvoeren van PIA's breder verplicht dan de AVG vereist
  - Investeer in de verdere ontwikkeling van het Toetsmodel

Voor optimaal effect moet de organisatie zelf voldoende betrokken zijn bij de PIA. Indien het uitvoeren wordt uitbesteed, kan deze betrokkenheid bereikt worden met bijvoorbeeld interviews of workshops.

5.2 Inhoud en vorm

Het Toetsmodel blijkt niet voor alle PIA's even geschikt te zijn. Eén oorzaak daarvan is dat het onvoldoende onderscheid maakt tussen enerzijds PIA's voor wetgeving of beleid, en anderzijds PIA's voor systemen of processen. Meer in het algemeen laat een verplichte vragenlijst te weinig ruimte voor eigen invulling door de verantwoordelijke. Verantwoordelijken hebben in onze ervaring als het gaat om privacywetgeving echter wel vaak behoefte aan houvast. Wij zien de oplossing in een verplicht kader voor het uitvoeren van en rapporteren over PIA's, aangevuld met modellen en handreikingen die aan dat kader nadere invulling geven. In het op te stellen kader dient een voldoende ruime plaats te zijn weggelegd voor twee essentiële inhoudelijke zaken die in het Toetsmodel te weinig aandacht krijgen: proportionaliteit en privacyrisico's.

Aanbevelingen

- Maak onderscheid tussen enerzijds PIA's voor wetgeving of beleid, en anderzijds PIA's voor systemen of processen.
- Stap af van een verplichte vragenlijst. Stel in plaats daarvan een verplicht kader op, en vul dat aan met onder meer een model-vragenlijst.

Gelet op de vorige aanbeveling kan het ook om twee model-vragenlijsten gaan. Een organisatie kan de model-vragenlijst in de aangeboden vorm hanteren, deze wijzigen of aanvullen, of een eigen vragenlijst ontwikkelen die voldoet aan de gestelde criteria.

- Neem keuzes en opties op in het kader, zoals de mogelijkheid om minder diep te gaan voor verwerkingen met beperkte privacyrisico's.
- Formuleer criteria waaraan de verslaglegging van een PIA hoort te voldoen, en voeg daaraan een model-opzet van een PIA-rapport toe.

Net als voor de model-vragenlijst geldt dat een organisatie de model-opzet in de aangeboden vorm kan hanteren, deze kan wijzigen of aanvullen, of een eigen opzet ontwikkelen die voldoet aan de gestelde criteria.

- Ruim in het kader voldoende plaats in voor het beoordelen van de proportionaliteit van de voorgenomen gegevensverwerking.
- Ruim in het kader voldoende plaats in voor het in kaart brengen en beoordelen van de privacyrisico's, en voor het vaststellen van de maatregelen die zullen worden genomen om die risico's te vermijden of tot een acceptabel niveau terug te brengen.

Het Toetsmodel blijkt ook niet voor alle uitvoerders van PIA's even geschikt te zijn. Velen hebben moeite met de uitgebreide tekst, het juridische jargon daarin en het gebrek aan voorbeelden. Een interactief, bijvoorbeeld via de browser, in te vullen versie van het Toetsmodel zou het gebruiksgemak eveneens aanzienlijk vergroten.

Aanbevelingen

- Maak het Toetsmodel gebruikersvriendelijker. Hou daarbij rekening met de diverse soorten gebruikers die het kent.
- Breid de (inhoudelijke) toelichting uit, onder meer door voorbeelden toe te voegen.
- Vermijd juridisch taalgebruik waar dat mogelijk is, en voeg een niet-juridische uitleg toe waar dat niet mogelijk is.

Het doel van deze twee aanbevelingen is niet om zij die geen privacydeskundige zijn in staat te stellen zelfstandig een PIA uit te voeren, wel om te bevorderen dat zij een optimale bijdrage kunnen leveren aan het PIA-proces.

- Ontwikkel een interactief, bijvoorbeeld via de browser, in te vullen versie van het Toetsmodel c.q. de model-vragenlijsten.

5.3 Proces

Organisaties blijken nogal eens moeite te hebben om het PIA-proces goed te laten verlopen. Dat begint met enerzijds de vraag beantwoorden wanneer er eigenlijk een PIA moet worden uitgevoerd, en anderzijds ervoor zorgen dat er ook een PIA gestart wordt als het antwoord op die vraag bevestigend luidt. Maar ook voor de rest van het proces is lang niet altijd duidelijk wat ieders taken en verantwoordelijkheden zijn of zouden moeten zijn. Dit is deels terug te voeren op onvoldoende privacy governance; het uitvoeren van PIA's moet echter niet afhankelijk zijn van versterkingen daarin. Organisaties hebben er daarom baat bij dat er naast een inhoudelijk kader ook een kader komt voor het PIA-proces. Ook hier dient de specifieke invulling vrijgelaten te worden, gelet op de verschillen in hoe organisaties werken. Wel kan er een model-PIA-proces worden aangeboden, en zou het mooi zijn als dat verweven kan worden in de model-vragenlijst, zodat de degenen die bij de PIA betrokken zijn als het ware vanzelf door het proces wordt geleid. Dat proces eindigt pas wanneer de organisatie verantwoording heeft afgelegd over wat zij met de uitkomsten van de PIA heeft gedaan, bij voorkeur zo breed mogelijk. En het hoort weer opnieuw opgestart te worden wanneer de gegevensverwerking of de risico's die daarmee gepaard gaan significant veranderen.

Privacywetgeving is complex en wemelt van de open normen. Bij het uitvoeren van een PIA is privacydeskundigheid daarom onontbeerlijk. 'Good practices' voor het PIA-proces zijn daarnaast het houden van PIA-workshops en het consulteren van stakeholders. Met dat laatste blijken organisaties moeite te hebben als het gaat om betrokkenen in de zin van de Wbp, dat wil zeggen personen van wie gegevens worden verwerkt.

Aanbevelingen

- Stel een verplicht kader op voor het uitvoeren van een PIA[26], en vul dat aan met bijvoorbeeld een model-PIA-proces.
- Aandachtspunten bij het opstellen van dat kader zijn:
  - Benoem bevoegdheden, rollen, taken en verantwoordelijkheden.
  - Neem op dat privacydeskundigheid onontbeerlijk is voor een goed PIA-proces.
  - Neem het houden van PIA-workshops op als 'good practice'.
  - Neem het consulteren van stakeholders op als 'good practice'.
  - Stel een handreiking op over het betrekken van betrokkenen (of organisaties die hen vertegenwoordigen).
  - Neem het belang op van transparantie over de uitkomsten van de PIA.
  - Neem het afleggen van verantwoording op over wat de organisatie gedaan heeft met de uitkomsten van de PIA.
  - Neem op dat de PIA geactualiseerd moet worden als de gegevensverwerking of de risico's die daarmee gepaard gaan significant veranderen.
  - Verwerk het model-PIA-proces zoveel mogelijk in de model-vragenlijst, zodat uitvoerders als het ware vanzelf door het proces worden geleid.
  - Werk nader uit wat de criteria zijn wanneer al dan niet een PIA moet worden gedaan, en vertaal die naar een "PIA Quick Scan" die organisaties helpt om deze vraag te beantwoorden.

26. Zie het eindrapport van het reeds genoemde PIAF-project, in het bijzonder paragraaf 3.3.

Referenties

Centrum voor Informatiebeveiliging en Privacybescherming,
“Privacy Baseline versie 1.0”, november 2015

College Bescherming Persoonsgegevens, brief aan Ministerie BZK
over Advies – concept Toetsmodel Privacy Impact Assessment, 5 maart 2013

EU PIAF Project, “Recommendations for a privacy impact assessment framework
for the European Union”. Deliverable D3, november 2012

Kamerstukken I 2010/11, 31 051, D (motie Franken c.s.)
Kamerstukken II 2012/13, 26 643,
nr. 282 en bijlage (aanbiedingsbrief, Toetsmodel, inclusief toelichting)
Kamerstukken I 2013/14, 31 051, G
(verslag van een schriftelijk overleg met de Eerste Kamer)
Kamerstuk II 2014/2015 34 000 VII nr. 21 (motie Segers/Oosenbrug)
Kamerstukken II 2014/15, 26 643 nr. 335
(brief in reactie op de motie van de leden Segers en Oosenbrug)
Kamerstuk II 2014.15 32 761 nr. 83 (visie op privacy)

Made, Mees van der. Praktische toets PIA helpt privacy beschermen.
BinnenbeRijk, Jaargang 10, nummer 2, mei 2014

Morijn, John. Notitie: Tussenevaluatie toepassing PIA Toetsmodel Rijksdienst.
Ministerie BZK, directie CZW, 14 juni 2014

UK Informations Commissioner’s Office,
“Conducting privacy impact assessments code of practice”, februari 2014

Wright, D. “Making Privacy Impact Assessment More Effective”,
The Information Society 29:5, p. 307-315, 11 oktober 2013

Bijlage I – Literatuur-onderzoek

1 Over het Toetsmodel PIA Rijksdienst

1.1 Relevante publicaties

Het aantal publicaties over het Toetsmodel is vrij beperkt. Wij zijn voor wat betreft relevante publicaties gekomen tot de volgende lijst:

- Kamerstukken I 2010/11, 31 051, D (motie Franken c.s.)
- Kamerstukken II 2012/13, 26 643, nr. 282 en bijlage (aanbiedingsbrief en Toetsmodel, inclusief toelichting)
- Kamerstukken I 2013/14, 31 051, G (verslag van een schriftelijk overleg met de Eerste Kamer)
- Kamerstukken II 2014/15 34 000 VII, nr. 21 (motie Segers/Oosenbrug)
- Kamerstukken II 2014/15, 26 643, nr. 335 (reactie op motie Segers/Oosenbrug)
- Kamerstukken II 2014/15, 32 761, nr. 83 (visie regering op privacy)
- "Tussenevaluatie toepassing PIA Toetsmodel Rijksdienst", Ministerie BZK, directie CZW, John Morijn, 14 juni 2014
- "Praktische toets PIA helpt privacy beschermen", Mees van der Made. BinnenbeRijk 10(2), mei 2014
- "Privacy Baseline versie 1.0", november 2015, Centrum voor Informatiebeveiliging en Privacybescherming

In aanvulling hierop hebben wij vanuit verschillende kanten toegang gekregen tot vertrouwelijke documenten die ons in staat hebben gesteld om ons beeld te toetsen en verder aan te scherpen.

1.2 Algemeen kader

Aan de hand van de bovenstaande literatuur zetten we de belangrijkste punten kort uiteen.

1.2.1 Ontwikkeling Toetsmodel (2011–2013)

In mei 2011 neemt de Eerste Kamer de motie Franken c.s. aan. Deze verzoekt de regering om voorstellen voor nieuwe wetgeving waarbij sprake is van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer te toetsen op, onder meer, "de resultaten van een Privacy Impact Assessment, zodat vooraf is onderzocht welke risico's de maatregel met zich meebrengt".

In juni 2013 bieden de Minister voor Wonen en Rijksdienst en de Staatssecretaris van VenJ aan de Tweede Kamer het Toetsmodel PIA Rijksdienst aan, met ingangsdatum 1 september 2013.[27] In juli 2013 hebben de leden van de vaste Kamercommissie voor VenJ hun reactie gegeven. De commissie gaf onder meer het volgende aan:

- Het Toetsmodel bevat alleen het risico-identificerende gedeelte van een PIA. Dit is een goede stap, maar een volledige PIA gaat verder; met een volledige PIA wordt er meer in kaart gebracht dan alleen de risico's. Ook de voorgestelde Europese Privacyverordening gaat uit van een volledige PIA. Met het invullen van het Toetsmodel worden dus niet alle privacy-eisen afgedekt.
- Voorts wordt er in het Toetsmodel onvoldoende rekening gehouden met de eisen die de voorgestelde Europese Privacyverordening gaat stellen; zo ontbreken de voorgestelde eisen van 'privacy by design' en 'privacy by default'.
- Tot slot leidt de beantwoording van belangrijke vragen uit het Toetsmodel niet in alle gevallen duidelijk tot bepaalde gevolgen. Daardoor lijkt het alsof de vragen eerder bedoeld zijn voor toepassing van de Wbp op geïnventariseerde verwerkingen dan voor risico-identificering voor de privacybescherming van betrokkenen.

- Een volgende versie van het Toetsmodel dient meer in overeenstemming gebracht te worden met de werkelijke bedoeling van een PIA alsook met de eisen die de te verwachten Europese Privacyverordening met zich meebrengt.

De Minister voor Wonen en Rijksdienst en de staatssecretaris van VenJ reageerden als volgt op de Commissie:

- Het Toetsmodel is slechts onderdeel van een veel breder, al bestaand instrumentarium om privacyaspecten van beleid- en wetgeving te toetsen, dat onverkort van kracht blijft. Een voorbeeld hiervan is de Leidraad afstemming wetgeving op de Wbp.[28]
- Er is bij de ontwikkeling van het Toetsmodel gekozen voor vragen die de juridische normen vertalen naar feitelijke vragen die in het beginstadium van beleidsvorming vaak spelen of andere informatie kan achterhalen die noodzakelijk is voor welafgewogen besluitvorming.
- Het Toetsmodel moet de verschillende bestaande toetsinstrumenten beter verbinden met de betrokken actoren (zoals FG's en CIO's).
- In artikel 35 lid 9 van de voorgestelde Europese Privacyverordening wordt de overheid expliciet uitgezonderd van de PIA-verplichting. De uitzondering hangt samen met de verwachting dat overheden bij ontwikkeling van wetgeving en beleid reeds waarborgen hanteren die privacyaspecten structureel toetsen.
- Met betrekking tot het niet opnemen van 'privacy by design' en 'privacy by default' geldt dat deze beide als technische oplossingen worden zien. Hoewel ze in elkaars verlengde liggen, spelen ze in een andere context. Beide liggen ten grondslag aan de opzet van de PIA-vragenlijst, maar om verwarring te voorkomen is ervoor gekozen om de termen niet letterlijk op te nemen. Door de PIA-resultaten naar de CIO's door te sturen, kunnen deze worden meegenomen bij de besluitvorming over de beveiligingsmaatregelen.
- Het Toetsmodel is zowel richtinggevend als sturend en corrigerend van aard. Hier is expliciet voor gekozen. Het voorkomt namelijk overlap met meer juridisch en technisch getinte toetsingsinstrumenten; bij toepassing van deze instrumenten zullen de uitkomsten van het Toetsmodel als input dienen (sturend). Het richtinggevende en corrigerende karakter sluit aan bij het basisdoel van het Toetsmodel: het vergroten van bewustzijn van verschillende privacyaspecten binnen de Rijksoverheid. Er wordt door de regering voorlopig geen reden gezien om deze aanpak te wijzigen.

1.2.2 Motie Segers en Oosenbrug en reactie Plasterk (november 2014)

De motie van de Tweede Kamerleden Segers en Oosenbrug (november 2014) verzocht de regering om bij nieuwe wetgeving met gevolgen voor de verwerking van persoonsgegevens PIA's uit te voeren, dan wel het ontbreken daarvan te motiveren.[29] In reactie daarop verwijst de Minister van BZK naar het Toetsmodel en de begeleidende stukken.[30] Ook geeft de Minister aan dat het Toetsmodel op dat moment nog niet altijd even consequent wordt toegepast en dat er bij nieuwe wetgeving nog niet altijd op een inzichtelijke manier verslag wordt gedaan van de resultaten van het Toetsmodel. Voorts noemt de Minister het onderhavige evaluatieonderzoek om de gevallen van en redenen voor het niet toepassen van het Toetsmodel te bekijken, evenals de wijze van verslaglegging van de resultaten in de memorie van toelichting.

1.2.3 Visie op privacy Minister van VenJ (mei 2015)

In mei 2015 heeft de Minister van VenJ gereageerd op een open brief aan hem waarin een 'privacycoalitie' van organisaties, bedrijven en personen haar zorgen uit over de privacybescherming van burgers in de informatiemaatschappij. Volgens dit Kamerstuk zijn er acht toetsstenen die in de visie van het kabinet bepalend moeten zijn voor het privacybeleid. Het Toetsmodel wordt in deze toetsstenen genoemd als zevende vraag, en luidt: *"Is er, waar nodig, een Privacy Impact Assessment (PIA) uitgevoerd?"*[31] De Minister geeft aan dat op deze vraag bij elk traject een deugdelijk antwoord geformuleerd dient te worden.

1.2.4 Advies AP over concept-Toetsmodel PIA (maart 2013)

Voorafgaand aan de invoering van het Toetsmodel PIA Rijksdienst heeft de AP toentertijd een advies opgesteld voor het instrument dat volgens de AP nauw verband houdt met de wettelijke adviestaak van het AP in artikel 51 lid 2 Wbp. De AP geeft aan dat ze uitgaat van een zeer positieve waardering voor het initiatief zelf, gelet op het belang van bewustzijn en nemen van verantwoordelijkheid voor een zorgvuldige verwerking van persoonsgegevens bij verantwoordelijken.

Naast het concrete advies benadrukt de AP dat een PIA geen compliancetoets is. De PIA-toets van het Toetsmodel is volgens de toezichthouder “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 leidinggevenden de risico’s in relatie tot bescherming persoonsgegevens op overzichtelijke wijze in kaart te brengen.”[32]

Twee aandachtspunten die de AP in haar brief herhaalt met het oog op een eerder initiatief van de concept-PIA die relevant zijn voor het Toetsmodel zijn de volgende. Het hele instrument dient te zijn geformuleerd in eenvoudige, toegankelijke taal, zonder jargon. Daarnaast dient de uitvoering van de PIA op zichzelf een duidelijk en autonoom resultaat op te leveren, zodat dat de uitvoerder weet waar bij zijn project de privacyrisico’s zitten.

De AP geeft 5 grondbeginselen voor een PIA:

1. Een 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.

De concrete aandachtspunten van de AP zien onder meer op het duidelijk maken van het moment waarop een PIA kan worden uitgevoerd. Ook benoemt de AP dat antwoorden kunnen worden volstaan met ja/nee zonder verdere toelichting, dat onvoldoende handvatten geeft aan beoordelaars voor het inschatten van de privacy risico’s voor betrokkenen. Daarnaast ziet het AP het concept-Toetsmodel als een compliance toets vormgegeven, vanwege het feit dat de Wbp-artikelen worden nagelopen. De Leidraad – afstemmen van wetgeving op de Wet bescherming persoonsgegevens wordt door de AP genoemd als het instrument om de juridische toets uit te voeren nadat de PIA is gedaan met het Toetsmodel. Tot slot gaat de AP ook in op de rol van de FG. Het gaat dan over een passage uit het concept-Toetsmodel die aangeeft dat bij vragen de uitvoerder contact kan opnemen met de FG (of CIO). De AP haalt het WRR-rapport “iOverheid” aan en adviseert nadere uitwerking te geven aan de rol die de FG intern heeft als toezichthouder versus intern adviseur. In het huidige Toetsmodel staat nog steeds dat de gebruiker bij onduidelijkheid over de inhoud van de vraag, contact kan opnemen met de eigen FG.

1.2.5 Tussenevaluatie Morijn (juni 2014)

Volgens Morijn lijkt aan de ene kant het Toetsmodel frequent te worden toegepast bij de ontwikkeling van nieuw beleid en wetgeving.[33] Bij het uitvoeren van het Toetsmodel is veelal de indruk dat een volledi ger beeld is gecreëerd van de privacyaspecten bij het nieuwe beleid of de nieuwe wetgeving, dan zonder het Toetsmodel verkregen zou worden. Ook wordt de uitvoering van een PIA bij de ontwikkeling van nieuw beleid en wetgeving door externe partijen ook steeds vaker als standaard verwacht.[34] Hiermee lijkt op het eerste gezicht dat het doel 'richting geven aan nieuw beleid en wetgeving' van het Toetsmodel wordt bereikt. Echter, anderzijds wordt geconstateerd dat de uitvoering van het Toetsmodel nog niet rijksbreed wordt uitgevoerd. Morijn somt een aantal gegeven redenen op:

'Dit is een Amvb, de basis voor gegevensverwerking ligt al in de bovenliggende wet en we gaan nog niet nog een keer een PIA doen', 'dit is een wet, maar we gaan de te gebruiken gegevens en/of doel specifiëren in een Amvb, we doen de PIA later', 'een ander departement moet het voortouw nemen, wij hebben niet de systeemverantwoordelijkheid', 'het is geen nieuw beleid, maar borduurt voort op ouder beleid', 'de oplossing voldoet al aan technische standaarden (bijv. NEN/ISO)', 'Het Cbp heeft in gesprekken/bij advisering niet om PIA gevraagd, de PIA komt nog, wordt extern geleverd, een PIA light is afdoende (terwijl niet aan de criteria wordt voldaan)', 'CZW/DWJZ-WKB zei dat privacy OK is, dat een PIA niet nodig was.'

Voorts constateert Morijn dat de politieke realiteit ook vaak is dat bijvoorbeeld een regeerakkoord (vooraf) aankondigt dat een gegevensverwerking zal worden ingevoerd of uitgewerkt. Het invullen van het Toetsmodel krijgt dan volgens hem meer het karakter van een exercitie om een onderbouwing te geven van een probleem waarvoor al een oplossing is bedacht. Richting geven is dan nog wel mogelijk, maar de corrigerende mogelijkheden van de PIA zijn in zulke gevallen beperkt.[35]

Morijn doet in zijn tussenevaluatie de volgende aanbevelingen:

- De noodzaak van het uitvoeren van een PIA moet binnen en vanuit wetgevingsafdelingen benadrukt worden. Ook moet er een toelichting voor en bij het Toetsmodel komen over het (verplicht) gebruik van het Toetsmodel, waardoor er voor (externe) partijen duidelijkheid komt wanneer het Toetsmodel wel of niet moet worden ingevuld en wiens verantwoordelijkheid het is (zodat de verantwoordelijkheid niet kan worden doorgeschoven).
- Er moet een uitleg (bijv. door middel van een cursus of flyer) komen over het praktisch aanpakken van het Toetsmodel, met daarin concrete handvatten.[36]
- Er moet op korte termijn een besluit komen of de resultaten van het Toetsmodel wel of niet standaard naar de Kamers worden gestuurd. Morijn raadt aan om dit wel te doen.
- Het Toetsmodel moet gezamenlijk worden ingevuld door medewerkers met privacykennis en beleidsmedewerkers. Enerzijds om de kwaliteit van het Toetsmodel te waarborgen, anderzijds om algehele privacybewustwording te creëren bij beleidsmedewerkers en hun input met betrekking tot de noodzakelijkheid van de gegevensverwerking te betrekken.[37]
- Er moet duidelijkheid worden geschept over de samenhang van en verhouding tussen de verschillende Toetsmodellen die in omloop zijn, met daarbij duidelijke criteria welk Toetsmodel in welke geval het beste kan worden gebruikt.[38]
- De rol en de verantwoordelijkheden van een FG en eventueel de RPPF[39] moet duidelijker worden gemaakt worden bij de uitvoering en controle van het Toetsmodel.[40]
- In de toelichting van het Toetsmodel moet gespecificeerd worden dat de focus van het Toetsmodel ligt op de informationele privacy (gegevensbescherming) en niet op andere vormen van privacy
- Aan de hand van het ingevulde Toetsmodel moeten de belangrijkste risico's gedestilleerd worden. Er dient nog bepaald te worden of hieraan in het Toetsmodel richting moet worden gegeven of dat dit de taak is voor de FGs en CIOs.

- Morijn beveelt aan dat er bekeken dient te worden of de reikwijdte van het Toetsmodel moet worden verbreed naar de gehele overheid. Zo ja, dan dient bekeken te worden of en hoe de verschillende Toetsmodellen op elkaar kunnen worden aangesloten en dienen er criteria opgesteld te worden die aangeven welk Toetsmodel het meest geschikt is voor welke situatie. Op die manier wordt een zo groot mogelijke privacynaleving gewaarborgd.
- Voorts dient bekeken te worden wat de verhouding en samenhang is van het Toetsmodel in het bredere plaatje van privacymaatregelen en de daarbij betrokken instrumenten en actoren. Denk hierbij bijv. aan privacy by design, privacy enhancing technologies en privacy by default.

1.2.6 BinnenbeRijk (mei 2014)

In een kort artikel uit BinnenbeRijk (vakblad voor bedrijfsvoering binnen het Rijk) van mei 2014 is er aandacht voor het Toetsmodel. In het stuk geeft de FG van het Ministerie van Economische Zaken, Jan de Zeeuw, aan op welke manier het Toetsmodel zou kunnen worden verbeterd. Zo komt het volgens hem nog voor dat de vragenlijst met te weinig diepgang wordt ingevuld waardoor de risico's onvoldoende aan het licht komen. In het proces zou daarom idealiter een privacydeskundige betrokken moeten worden, zeker als het gaat om een rijksbreed project. "In een ideale situatie hoef je als projectleider maar één telefoontje te plegen, naar een soort expertisecentrum persoonsgegevens, waar een expert jouw PIA direct kan begeleiden."[41] Auke Bloembergen (adviseur bij PBLQ) geeft aan dat het Toetsmodel goed heeft geholpen bij de ontwikkeling van het Rijks Identificerend Nummer (RIN). Zo beschrijft hij dat de PIA heeft geholpen om een aantal specifieke beslissingen te nemen met betrekking tot de bewaartermijn en minimalisatie van persoonsgegevens. "Het aantal gegevens, dat nodig is om een RIN [Rijks Identificerend Nummer] aan te maken voor een medewerker, [is] dankzij PIA tot een minimum beperkt."[42]

In aanvulling op het bovenstaande, heeft Jan de Zeeuw een aantal concrete aandachtspunten met betrekking tot de huidige vorm van het Toetsmodel met ons gedeeld. Zo merkt hij op dat een ingevulde PIA niet altijd bruikbaar is als resultaat. Dat komt mede omdat de belangrijkste vragen niet altijd als zodanig worden herkend. Het komt dan ook vaak voor dat veel tekst en flowcharts niet relevant zijn, terwijl andere informatie juist te moeilijk blijkt om te achterhalen. De Zeeuw ziet mogelijkheden in het aanreiken van een FG of andere deskundige die vooraf sturende deelvragen kan aanreiken.

Procesmatig zijn er volgens De Zeeuw problemen met betrekking tot de besluitvorming. De uitkomst van de PIA is daarvoor veelal niet noodzakelijk. Beslissingsmomenten lopen daarom niet synchroon met het gereedkomen van het resultaat van de PIA. Dit vindt deels zijn aard in de situatie dat de plicht voor het uitvoeren van de PIA niet ook behelst dat de PIA betrokken moet worden in de besluitvorming. Dat werpt tijdens projecten vragen op over of een besluit alsnog geïmplementeerd kan worden zonder volledig uitgevoerde PIA. Daarnaast is ook onduidelijk of de verplichte PIA ook van toepassing is op beleid/systemen van vóór 1 september 2013 of überhaupt wanneer de verplichting wel en niet geldt.
Met betrekking tot het toezicht op het Toetsmodel is het volgens De Zeeuw onbekend wie verantwoordelijk is over de uitvoering van de PIA op rijksbrede onderwerpen. Daarnaast is punt van aandacht hoe kwaliteit en vooruitgang geborgd worden als de antwoorden lastiger worden. Ook is het richtinggevende en corrigerende karakter van de PIA niet heel duidelijk. Daarom is een van de vragen ook hoe het resultaat van de PIA er uit dient te zien, moet dit een document met alleen antwoorden te zijn of moet dit document bijv. ook afwegingen, alternatieven keuzes en/of daadwerkelijke aanbevelingen bevatten?

Concluderend geeft De Zeeuw aan dat de verplichting en de brede inzetbaarheid zeer welkom zijn. Maar dat het richtinggevende dan wel corrigerende karakter én de noodzakelijkheidstoets dwingend onderdeel van het beantwoordingsschema hoort te zijn. Ook zou een manier gevonden moeten worden om het doel van een serieus uitgevoerde PIA altijd te bereiken. Daartoe kan bijdragen: het duidelijk voorschrijven van een te behalen resultaat en het inschakelen van privacydeskundigen. Bewustwording is volgens De Zeeuw een welkome uitkomst van de PIA, maar er is met name behoefte aan (rijksbreed) beleid en tools voor privacy.

1.2.7 De Privacy Baseline van het CIP (november 2015)

Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) heeft een Privacy Baseline opgesteld. Hierin is de Wet bescherming persoonsgegevens (Wbp) vertaald naar concrete normen en te nemen maatregelen in het beleidsdomein, uitvoeringsdomein en control/beheerdomein. Ten behoeve van de Baseline is onder meer het Toetsmodel geëvalueerd. Op basis daarvan heeft het CIP onder meer het volgende geconcludeerd. Middels het Toetsmodel kan de overheid de risico's van voorgenomen wetgeving of beleid in kaart brengen. Op basis van de uitkomsten kan de overheid bepalen welke beveiligingsmaatregelen passend en nodig zijn om de betreffende risico's te verminderen of weg te nemen. Uit het Toetsmodel zelf blijkt echter niet welke concrete maatregelen er genomen moeten worden. Voorts maakt het Toetsmodel niet duidelijk wat er concreet waar geregeld moet worden om volledig aan de Wbp te voldoen. Het Toetsmodel brengt 'slechts' risico's in kaart en hoewel dit zeer nuttig is (en ook noodzakelijk voor het nemen van beveiligingsmaatregelen), wordt hiermee niet volledig aan de Wbp voldaan, omdat de Wbp meer eist dan alleen risico-beheersing. Voorts brengen PIA's niet van elke Wbp-eis de risico's in kaart. Er ontbreken vragen over een aantal belangrijke eisen van de Wbp, zoals vragen over:

- De gronden voor verwerking (waaronder opslag en doorgifte) in landen buiten de EU;
- De rechtvaardigingsgronden voor verdere verwerking als de verenigbaarheid ontbreekt;
- Transparantie voor eenieder over de gegevensverwerkingen;
- De schriftelijke bewerkersafspraken. In het Toetsmodel wordt de bewerkersovereenkomst alleen ergens kort in de toelichting genoemd, terwijl schriftelijke bewerkersafspraken verplicht en erg belangrijk zijn.
- Sectorspecifieke wetgeving op andere onderwerpen dan (op dit moment alleen behandelde) bewaartermijnen.

Verder zijn het nut en de achterliggende gedachte van sommige vragen niet altijd even duidelijk. Zo stelt het Toetsmodel de vraag of er gegevens worden verwerkt over 'kwetsbare groepen of personen'; de Wbp zegt hier niets over en het Toetsmodel geeft geen nadere uitleg waarom deze vraag gesteld wordt en wat voor consequenties daaraan moet worden verbonden. Voorts merkt het CIP op dat er diverse PIA's zijn. Momenteel is het voor organisaties soms lastig te beoordelen welke PIA waarvoor geschikt is en voor welke PIA er in een concreet geval moet worden gekozen.

2 Essentiële kenmerken Privacy Impact Assessments

2.1 'Best practices'

De afgelopen decennia is er veel gepubliceerd over Privacy Impact Assessments. Er zijn twee leidende publicaties die kennis op het gebied van PIA's hebben gecomprimeerd. Dit zijn van de "Recommendations for a privacy impact assessment framework for the European Union" van het door de EU gefinancierde project PIAF, en de "Conducting privacy impact assessments code of practice." van de ICO.[43] In aansluiting op deze publicaties hebben we recentere publicaties meegenomen in het destilleren van de essentiële kenmerken van een PIA.

2.1.1 Het waarom van een PIA

Een PIA is een instrument waarmee organisaties mogelijke privacyrisico's in kaart kunnen brengen. Een PIA kan bij diverse zaken worden uitgevoerd, bijvoorbeeld bij de ontwikkeling van een nieuw bedrijf, product, systeem, dienst, wetgeving of beleid. Op basis van de uitkomsten van een PIA kunnen organisaties concrete organisatorische, technische en fysieke beveiligingsmaatregelen nemen om de risico's te mitigeren of elimineren. Hoe eerder een PIA wordt uitgevoerd, hoe beter. Allereerst omdat hierdoor tijdig maatregelen kunnen worden genomen die zo veel als mogelijk voorkomen dat de risico's (voor zowel burgers als organisatie) zich überhaupt voordoen. Daar komt bij dat het ook eenvoudiger en goedkoper is om vooraf maatregelen in te regelen dan om achteraf een bedrijf, systeem, product, beleid of wetgeving aan te passen, ook gelet op eventuele boetes, te betalen schadevergoeding en reputatieschade die tussentijds kunnen optreden. Ook kan het uitvoeren van een PIA bijdragen aan privacybewustzijn binnen de organisatie, en aan een betere verstandhouding tussen burger en organisatie (doordat de burger meer vertrouwen in de organisatie krijgt).

2.1.2 De kwaliteit van de PIA

De kwaliteit van de PIA dient geborgd te worden. Dit kan worden bewerkstelligd door specifieke, deskundige personen aan te wijzen die verantwoordelijk zijn voor het uitvoeren van de PIA.

Een PIA bestaat uit meerdere onderdelen c.q. aspecten, waarvan een juridische compliancetoets er een kan zijn (maar ook niet meer dan dat). Wettelijke kaders vormen de basis voor het waarborgen van privacy en dienen aangevuld te worden met technische en organisatorische maatregelen. Om de kwaliteit van de uitkomsten van de PIA te borgen kan het helpen als het PIA-instrument een gedegen suggestie doet met betrekking tot de structuur van het eindresultaat.

2.1.3 De PIA als proces

Het PIA-proces dient te waarborgen dat mogelijke risico's in een vroeg stadium worden onderkend. Het adresseren van de problemen in een vroeg stadium heeft als voordeel dat het eenvoudiger is en minder kosten met zich meebrengt. De procesbenadering houdt ook in dat de toelichting bij de PIA aangeeft dat deze meer is dan louter een compliancetoets. Ook kan het zijn dat een PIA meerdere keren dient te worden uitgevoerd, bijvoorbeeld bij de wijziging van een systeem, product of dienst. Wijzigingen kunnen namelijk nieuwe risico's met zich mee brengen en deze moeten ook in kaart worden gebracht zodat bijvoorbeeld de nodige beveiligingsmaatregelen genomen kunnen worden.

2.1.4 Beschrijving van project en gegevensstromen

Bij het uitvoeren van en rapporteren over een PIA moet duidelijk beschreven worden waarop de PIA precies betrekking heeft. Dat kan onder meer een project, product, systeem, bedrijf, beleid of wetgeving zijn. Het is belangrijk om dit in kaart te brengen zodat er een goed, volledig en concreet beeld ontstaat met alle relevante aspecten. Om welke bestanden en gegevensstromen gaat het, welke gegevens worden er door wie verwerkt, met welk doel, hoe lang enz.

2.1.5 Privacyrisico-identificatie

Door het uitvoeren van een PIA worden privacyrisico's en gerelateerde risico's in kaart gebracht. De PIA zou uiteindelijk een overzicht moeten opleveren van de privacyrisico's die samenhangen met het traject in kwestie. Dit moet onder meer helpen voorkomen dat er te veel, te weinig of onjuiste gegevens worden verzameld en verwerkt, of dat de gegevens in verkeerde handen vallen. Als er te veel gegevens worden verzameld en verwerkt, kan dit leiden tot profiling, mogelijk met discriminatie en stigmatisering tot gevolg. Ook moet voorkomen worden dat er onjuiste of onvoldoende gegevens over iemand worden verzameld of verwerkt omdat er zo een onjuist beeld van de betrokkene kan ontstaan. Als bijvoorbeeld een bank alleen schuldgegevens en geen inkomensgegevens verzamelt, dan kan het gebeuren dat een hypotheek wordt geweigerd terwijl de persoon in kwestie uitstekend in staat is om de hypotheek af te lossen.

2.1.6 Consultatie van stakeholders

Bij het uitvoeren van een PIA dienen interne en externe stakeholders te worden betrokken. Stakeholders zijn alle personen en organisaties die op enigerlei wijze belang hebben bij de gegevensverwerking in kwestie of bij de privacybestendigheid daarvan. Het betrekken van stakeholders stelt de uitvoerders van de PIA in staat om de zorgen die spelen in kaart te brengen en tegelijkertijd transparant te zijn over de gegevens die verwerkt zullen gaan worden en de redenen daarvoor.

2.1.7 Beoordeling van privacyrisico's

De PIA dient de privacyrisico's niet alleen in kaart te brengen. Het beoordelen van die risico's is een integraal onderdeel van een PIA. Voor het bepalen van de maatregelen die nodig zijn om de risico's (voldoende) weg te nemen is een balansoefening nodig.

2.1.8 Aanbevelingen formuleren

Als resultaat van het uitvoeren van de PIA dienen er aanbevelingen te worden geformuleerd. Deze aanbevelingen zien op maatregelen die nog genomen moeten worden. Daarbij dient ook te worden aangegeven welke organisatie of persoon ervoor verantwoordelijk is dat de aanbeveling (indien overgenomen) ook daadwerkelijk wordt uitgevoerd.

2.1.9 Vastlegging en goedkeuring door senior management

De resultaten van de PIA dienen vastgelegd te worden. Daarnaast is goedkeuring door de beleids- of systeemverantwoordelijke (senior management) een voorwaarde voor bestuurlijke borging.

2.1.10 Onafhankelijke beoordeling of audit van de resultaten

Het PIA-beleid dient te waarborgen dat er een (door een derde uitgevoerde) onafhankelijke beoordeling of audit van het PIA-rapport plaatsvindt.

2.1.11 Resultaten en aanbevelingen implementeren

De resultaten en aanbevelingen van het PIA-rapport dienen daadwerkelijk geïmplementeerd te worden in het ontwikkelingsproces van het beoordeelde project, dienst, product, bedrijf, beleid of wetgeving.

2.1.12 Publicatie PIA-rapport

Het PIA-instrument dient het publiceren van de resultaten aan te moedigen met het oog op transparantie. Hoewel er altijd bepaalde gevoeligheden in een PIA-rapport kunnen staan, is het volgens de literatuur aan te raden zo veel mogelijk transparant te zijn over de gegevensverwerkingen én de achterliggende risico-inschattingen.

2.2 De verhouding tot het huidige Toetsmodel PIA Rijkdienst

Aan de hand van in de vorige paragraaf beschreven essentiële kenmerken, gaan we in deze paragraaf kort in op wat we kunnen constateren met betrekking tot het Toetsmodel PIA Rijksdienst.

2.2.1 Het waarom van het Toetsmodel

Het uitvoeren van het Toetsmodel PIA Rijksdienst is voor de Rijksoverheid verplicht gesteld bij de ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien. Op dit moment geeft de toelichting bij het Toetsmodel het waarom van de PIA summier aan, maar wordt niet de nadruk gelegd op de voordelen die een dergelijke PIA kan bewerkstelligen. Een dergelijke toevoeging kan helpen bijdragen aan de bewustwording. Daarnaast ontbreekt een indicatie wanneer een PIA *niet* verplicht is.[45]

2.2.2 De kwaliteit van het Toetsmodel

In de toelichting bij het Toetsmodel wordt de beleidsmedewerker of wetgevingsjurist aangewezen als uitvoerder van de PIA. Het blijkt echter dat de kwaliteit van de PIA hierdoor onvoldoende wordt geborgd. Eén probleem is dat de uitvoerders van een PIA niet altijd over voldoende juridische kennis beschikken om de meer juridisch getinte onderdelen van het Toetsmodel inhoudelijk juist, volledig en relevant te beantwoorden. Ook geeft het Toetsmodel geen indicatie hoe een rapportage van een PIA er uit zou kunnen of moeten zien.[46]

2.2.3 Het Toetsmodel als proces

De toelichting van het Toetsmodel geeft aan dat een PIA zo vroeg mogelijk in het proces moet worden gebruikt. Echter wordt er verder geen consequentie aan verbonden als dit niet gebeurt. Ook de duiding van het Toetsmodel, waarom is het géén afvinklijst, kan in de toelichting beter omschreven worden.

2.2.4 Beschrijving van project en gegevensstromen

Het Toetsmodel bevat enkele concrete vragen om inzicht te krijgen op welke gegevens worden verwerkt en aan wie verstrekking plaatsvindt (vraag 1, 14 en 18). Een startvraag die op algemeen niveau vraagt wat het project inhoudt ontbreekt maar zou juist van toegevoegde waarde kunnen zijn om het Toetsmodel in een breder verband te zien én als een essentieel onderdeel van het project.

2.2.5 Privacyrisico-identificatie in het Toetsmodel

Middels de vragenlijst van het Toetsmodel worden er diverse gegevens opgevraagd, bijvoorbeeld om welke persoonsgegevens het gaat, of er een overzicht is of opgesteld kan worden van de gegevensstromen, hoe het staat met de beveiligingsmaatregelen en of het beleid is gericht op gegevensbescherming en-beveiliging. Deze zaken worden echter niet geduid in termen van privacyrisico's.

2.2.6 Consultatie van stakeholders

In het huidige Toetsmodel is niet opgenomen dat stakeholders gedurende de looptijd van het project/het opstellen van beleid- en wetgeving worden geconsulteerd. Wel kan er eventueel met de algemene consultatie bij wetgeving, waar reeds ook privacyaspecten aan bod komen, het een en ander worden gecombineerd.

2.2.7 Het beoordelen van privacyrisico's

Het Toetsmodel geeft momenteel geen handvatten voor het in kaart brengen van de privacyrisico's. De ervaring leert dat door het ontbreken van (voldoende) privacykennis bij de uitvoerder van de PIA de antwoorden op de vragen niet bruikbaar zijn als basis voor een gedegen risicobeoordeling.

2.2.8 Aanbevelingen formuleren

De toelichting geeft aan dat de FG, na de ontvangst van het PIA-rapport, mee kan helpen aan het formuleren van aanbevelingen. Het Toetsmodel geeft echter geen concrete of inhoudelijke aanwijzingen voor de wijze waarop aanbevelingen moeten worden geformuleerd.

2.2.9 Vastlegging en goedkeuring door senior management

De resultaten van de PIA worden in de praktijk standaard vastgelegd. De documentatie dient immers naar de FG (en soms ook de CIO) verstuurd te worden. Het Toetsmodel of de toelichting spreekt echter nergens over het laten accorderen van het resultaat door de persoon die verantwoordelijk is voor het beleid, wetgevingstraject of systeem.

2.2.10 Onafhankelijke beoordeling of audit van de resultaten

Het Toetsmodel bevat geen expliciete bepalingen over een onafhankelijke beoordeling van de resultaten van een PIA. Wel zegt de toelichting dat het PIA-rapport moet worden toegezonden aan de FG. Dat gebeurt echter niet altijd, en als het wel gebeurt dan gaan FG's op verschillende manieren met de resultaten om. Sommige zien geen rol voor zichzelf weggelegd, andere een beperkte. Geen enkele FG lijkt de wens te hebben of te beschikken over de middelen om alle ontvangen PIa-rapportages grondig door te lichten.

2.2.11 Resultaten en aanbevelingen implementeren

De toelichting bij het Toetsmodel geeft aan dat de resultaten van de PIA, afhankelijk van de wijze van uitvoering van de PIA, op verschillende manieren kunnen worden geïmplementeerd ("verwerkt") door de FG of CIO. De verantwoordelijkheid voor het implementeren van privacybeheersmaatregelen zal in de meeste gevallen echter elders liggen, of althans behoren te liggen.

2.2.12 Publicatie PIA-rapport

Het Toetsmodel zelf noch de toelichting daarbij gaat in op de mogelijkheid om het PIA-rapport openbaar te maken met het oog op transparantie. Wel bevat de toelichting een modeltekst die kan worden opgenomen in de Memorie van Toelichting van een wetsvoorstel. De bereikte transparantie hangt bij gebruik van die modeltekst sterk af van de wijze waarop deze wordt toegesneden op het traject in kwestie.

27. Kamerstuk EK 31 051, F.
28. Hoewel niet genoemd in de brief van de bewindslieden, bestaat er ook de Handleiding Wbp van het Ministerie van Justitie uit 2002, en ook het IAK (Integraal Afwegings Kader) bevat diverse checklists voor het toetsen van wetgeving aan grond- en mensenrechten. Daarnaast verwijzen we ook naar de Aanwijzingen voor de regelgeving, par. 4.11 over informatievoorziening en gegevensverwerking (aanwijzingen 161, 162, 162a en 162b).
29. Kamerstuk II 2014/2015 34 000 VII nr 21 (motie Segers/Oosenbrug).
30. Kamerstukken II 2014/15, 26 643 nr. 335 (reactie op motie Segers/Oosenbrug).
31. Kamerstuk II 2014.15 32 761 Nr 83 (visie op privacy).
32. College Bescherming Persoonsgegevens, brief aan Ministerie BZK over Advies – concept Toetsmodel Privacy Impact Assessment, 5 maart 2013.
33. Voorbeelden van wetgeving waarbij het Toetsmodel is uitgevoerd zijn onder meer de Jeugdwet, het Nationaal Detectienetwerk, de Wet regulering prostitutie en bestrijding van misstanden in de seksbranche, en het eID-stelsel.
34. Zo blijkt uit gesprekken met FG's dat de Autoriteit Persoonsgegevens (AP) steeds vaker om een ingevulde PIA-vragenlijst als er nieuwe wetgeving ter consultatie wordt opgestuurd en dat de AP soms niet wilde adviseren als de PIA nog niet klaar was.
35. Het uitvoeren van en rapporteren over een PIA heeft volgens Morijn daarmee nadrukkelijk ook een politieke dimensie.
36. Dit kan via het opzetten van een cursus en of brochure ter verduidelijking van een praktische aanpak. Hierin moeten praktische punten duidelijk gemaakt worden, bijvoorbeeld hoelang een PIA-proces moet duren, hoe stakeholders betrokken moeten worden, hoe de resultaten van de PIA naar risico's moeten worden omgezet en wanneer de FG betrokken moet worden. Indien er is besloten om extern in te kopen, zijn duidelijke instructies gewenst op grond van welke vragenlijst de analyse moet worden verricht.
37. Diverse FG's hebben aangegeven dat de inhoudelijke kwaliteit van de beantwoording van de vragenlijst lastig en vaak zodanig karig is dat een goede risico-inschatting niet mogelijk is. Bij het ontbreken van privacykennis bij de invulling van het Toetsmodel beperkt dit het richtinggevende en corrigerende effect van het ingevulde Toetsmodel. Hiernaast heeft dit veelal een lange reeks van communicatie tussen FG's en beleidsmedewerkers tot gevolg. Naast aanwezigheid van privacykennis is privacybewustwording binnen—en de noodzaak van input van—beleidsafdelingen (met betrekking tot het maken van beleidsrelevantie noodzakelijkheidstoetsing) van belang. De beleidsafdelingen dienen betrokken te worden bij het invullingsproces.
38. Het is positief dat er verschillende Toetsmodellen zijn, maar die zorgen in de praktijk weleens tot verwarring.
39. Bij Rijksbrede verwerkingen.
40. Bijv. waar begint en eindigt de verantwoordelijkheid.
41. Made, Mees van der, 2014. p. 14.
42. Made, Mees van der, 2014. p. 14.
43. De ICO (Information Commissioner's Office) is het Britse pendant van de Autoriteit Persoonsgegevens.
44. Aanbiedingsbrief Toetsmodel PIA-Rijksdienst, 21 juni 2013, van de Minister voor Wonen en Rijksdienst (S.A. Blok) en de staatssecretaris van Veiligheid en Justitie (F. Teeven).
45. Vgl. de opmerkingen van J. de Zeeuw in paragraaf 1.2.6 van deze bijlage.
46. De modelbeschrijving voor de paragraaf die opgenomen dient te worden in de Memorie van Toelichting geeft daarvoor ook geen houvast.

Bijlage II – Interviews

Ter evaluatie van het Toetsmodel PIA Rijksdienst hebben we geprobeerd om ons in de interviews een zo breed mogelijk beeld te vormen van de huidige situatie door verschillende functies en onderdelen bij de overheid te bevragen. De interviews hebben wij volgens een vast stramien afgenomen om zo goed mogelijk de verschillen en overeenkomsten tussen de functies en onderdelen van het Rijk te kunnen ontdekken. We verwijzen naar bijlage V voor een overzicht van de personen die geïnterviewd zijn.

Achtereenvolgens komen in dit hoofdstuk de volgende aspecten aan de orde:
- de wijze waarop de geïnterviewden bij PIA's betrokken zijn geweest
- het uitvoeren van een PIA
- de inhoud van het Toetsmodel
- het PIA-proces
- verslaglegging over de PIA
- effect van de PIA

In de interviews hebben wij gevraagd naar zowel de feitelijke ervaringen met het Toetsmodel en met het uitvoeren van PIA's in het algemeen, als naar ideeën en suggesties van geïnterviewden voor hoe het beter of anders zou kunnen.

De kwantitatieve gegevens hieronder dienen met enige terughoudendheid geïnterpreteerd te worden, zowel vanwege de relatief beperkte en niet geheel a-select samengestelde groep van geïnterviewden als vanwege de soms grote spreiding in de antwoorden.

1 Betrokkenheid geïnterviewde bij PIA's

De hoeveelheid PIA's waar geïnterviewden bij betrokken zijn geweest varieert nogal. Sommigen waren betrokken bij slechts een enkele PIA, terwijl dat aantal voor enkele anderen op meerdere tientallen ligt.

Meestal hadden de geïnterviewden een uitvoerende rol, maar ook de beoordelaarsrol werd vaak vervuld. Onder de geïnterviewden zaten relatief weinig opdrachtgevers.[47] Deze resultaten zijn goed te verklaren. Bij de uitvoerende rol bleek er vaker sprake van een eenmalige betrokkenheid, terwijl beoordelaars over het algemeen meer PIA's zien langskomen. Ook speelt mee bij welk ministerie de geïnterviewden werkzaam zijn.

De geïnterviewden hebben veelal PIA's uitgevoerd op wetgeving (in ontwikkeling) en in mindere mate op beleid. PIA's op (nog te ontwikkelen) systemen kwamen het minst vaak voor.[48] Uit de interviews kwam als mogelijke verklaring voor het lagere aantal systeem-PIA's naar voren dat systemen vaak al eerder dan de invoering van het Toetsmodel zijn opgezet en (al dan niet) getoetst. Ook genoemd werd de vermoedelijke onbekendheid met het feit dat bij het koppelen, aanpassen of anders gaan gebruiken van bestaande systemen. Dat dit minder speelt als het gaat om beleid of wetgeving kan te maken hebben met het door BZK voorgeschreven Integraal Afwegingskader voor beleid en regelgeving (IAK), dat de uitvoerder stapsgewijs langs het Toetsmodel leidt.

Diverse geïnterviewden merkten bovendien op dat zij het Toetsmodel niet of onvoldoende geschikt vinden voor het uitvoeren van PIA's op systemen. Dit hangt volgens hen samen met de (te) formele dan wel juridische formulering waardoor de vragenlijst in het Toetsmodel in sommige gevallen niet op praktijksituaties (denk aan nog te ontwikkelen systemen) is toegesneden. Een substantieel deel van hen pleitte daarom voor verschillende vragenlijsten, toegespitst op wetgeving en beleid dan wel op

(IT-)systemen en processen. Deze opinie werd overigens niet door iedereen gedeeld, enkele geïnterviewden zijn juist geen voorstander van een dergelijke scheiding, vooral omdat zij belang hechten aan een uniforme PIA-benadering binnen het Rijk.

2 Uitvoering PIA

De fase van uitvoering van de PIA blijkt redelijk gelijk verspreid te zijn geweest over drie fase-categorieën, namelijk: (1) voorafgaand aan dan wel in de voorfase van het project; (2) tijdens de projectontwikkeling of tijdens het project zelf (niet in de eindfase); en (3) in de eindfase. De vierde fase (na afloop van het project) was in veel mindere mate gebruikelijk, maar is wel eens voorgekomen. Laatstgenoemde situatie kan leiden tot zeer lastige kwesties, maar kan onvermijdelijk zijn wanneer er bijvoorbeeld ten onrechte geen PIA is gedaan en er vervolgens vanuit de maatschappij of de politiek vragen zijn gesteld bij de verwerking. Een concreet probleem dat zich dan kan voordoen is dat de persoon die achteraf een PIA doet (bij wijze van herstelactie) samen zal moeten werken met degenen die in een eerder stadium privacyaspecten inhoudelijk onvoldoende of onjuist beoordeeld hebben.

Verschillende geïnterviewden gaven expliciet aan dat het uitvoeren van een PIA in hun ervaring vooral symbolische waarde heeft, waarbij het door uitvoerders veelal wordt gezien als een compliancetoets (afvinklijst). In enkele gevallen werd bij het uitvoeren van een PIA op een andere benadering aangestuurd door privacydeskundigen indien deze aanwezig waren en betrokken waren bij de PIA. De FG (soms met vereende krachten vanuit andere departementen) kon soms ook tijdens of na het uitvoeren van de PIA bijsturen wanneer in het PIA-rapport niet de (werkelijke) volledige risico's in kaart waren gebracht. De aanpak die vanuit de privacydeskundigen op de werkvloer zelf werd gehanteerd, dus on-the-spot begeleiding, staat in nauw verband met het uitvoeren van de PIA (ruim) voor de eindfase van het project. Bij interventies vanuit de FG is dit verband minder sterk en kon het ook gebeuren dat er na afronding opnieuw naar een PIA moest worden gekeken. Een enkele keer leidde ook feedback van de AP tot een verbetering van een reeds uitgevoerde PIA.

Bij ongeveer de helft van de PIA's blijkt gebruik te zijn gemaakt van het Toetsmodel. De andere helft beslaat diverse alternatieve PIA-instrumenten, zoals die van de SURF, NOREA en de Belastingdienst. Het komt ook voor dat het Toetsmodel wel als uitgangspunt wordt gebruikt, maar er daarna een eigen vervolg aan wordt gegeven door middel van extra vragen of uitwerkingen. Aangegeven wordt dat er ook gebruik wordt gemaakt van een zelfgemaakte mix tussen vragen van het Toetsmodel en bijvoorbeeld de PIA van NOREA. De reden voor een keuze voor iets anders dan het Toetsmodel ligt hem in de ervaring dat het Toetsmodel tot te veel vragen leidt bij het gebruik ervan.

Daarnaast is aangegeven dat er soms een combinatie plaatsvindt met andere modellen, met ook andere doeleinden. Hierbij kan het gaan om vragenlijsten die zien op inventarisatie van verwerkingen, waarna er per verwerking concrete verbeteracties kunnen worden vastgesteld. Het Toetsmodel wordt dus soms aangevuld (vooraf met inventarisaties van verwerkingen, achteraf met risicoanalyses) en soms vervangen (vanwege het te juridische taalgebruik of de te abstracte vragen).

In de meeste gevallen werden de PIA's grotendeels uitgevoerd door eigen mensen; slechts in enkele gevallen hadden externe adviseurs de overhand. Enkele geïnterviewden noemen als argument voor het intern uitvoeren van een PIA dat dit bijdraagt aan de bewustwording op privacyvlak bij de betrokken medewerkers. Tijdens de interviews kwam ook naar voren dat bij het uitbesteden van een PIA soms nog wel eens problemen ontstaan. Zo is het voorgekomen dat bij een inkoopadviseur onvoldoende duidelijk was dat het uitvoeren van een PIA niet door een IT Auditor gedaan kan worden omdat die de specialistische privacykennis mist.

De geïnterviewden is ook gevraagd naar het aantal bestede uren aan de uitvoering van een PIA. De mediaan ligt rond de drie werkdagen. Het kwam regelmatig voor dat er tussen de 10 en 30 uur aan een PIA werden besteed, en geregeld werden er tussen de 30 en 100 uur besteed aan een PIA. Het kwam weinig voor dat er minder dan 10 of meer dan 100 uren aan een PIA werden besteed. Het aandeel van privacydeskundigen hierin bedraagt gemiddeld ongeveer de helft van het totale aantal uren.

3 Inhoud Toetsmodel

De geïnterviewden kregen enkele stellingen voorgelegd inzake de inhoud van het Toetsmodel. Hen werd gevraagd om een cijfer toe te wijzen op de volgende schaal:

1. volledig mee oneens
2. mee oneens
3. enigszins mee oneens
4. enigszins mee eens
5. eens
6. volledig mee eens

Stelling 1: de vragen van het Toetsmodel zijn op de praktijk toegesneden

2.5 *(tussen 'mee oneens' en 'enigszins mee oneens')*

Van alle stellingen werd de praktijkgerichtheid van het Toetsmodel het slechtst beoordeeld, de hoogste score die het Toetsmodel heeft gehaald op dit punt was een 4 (enigszins mee eens). Dit hangt onder andere samen met het aangekaarte taalgebruik (te 'juridisch') van het Toetsmodel en de Toelichting. Volgens sommigen 'past' het Toetsmodel minder goed voor een PIA op een (nog te ontwikkelen) systeem. Daarnaast is ook een aanleiding dat het Toetsmodel volgens geïnterviewden onvoldoende houvast geeft om risico's vast te stellen en om beveiligingsmaatregelen te bepalen.

Een andere ervaring was dat in overleg met FG kon blijken dat er andere (of meer) informatie gewenst was over bepaalde aspecten, die niet in het Toetsmodel werd uitgevraagd (of niet goed waren beantwoord in het resultaat van de PIA). Met deze achtergrond werd geopperd dat de modellen wellicht per departement aan de wensen van de FG zou moeten worden aangepast.

Stelling 2: de vragen van het Toetsmodel zijn begrijpelijk

3 *(enigszins mee oneens)*

Een groot deel van de geïnterviewden (ruim de helft) geeft aan dat problemen met de begrijpelijkheid van het Toetsmodel te maken hebben met de in hun ogen te juridische c.q. theoretische formuleringen die het hanteert. De toelichting ondervangt dit probleem naar hun mening op dit moment onvoldoende. Beleidsmedewerkers of PIA-uitvoerders die geen toegang hebben tot privacydeskundigheid blijken namelijk regelmatig moeite te hebben met het uitvoeren van een PIA aan de hand van het Toetsmodel.[49] Verwerkingen en hun context kunnen zelfs zo complex zijn dat ook privacydeskundigen niet de gewenste duidelijkheid kunnen verschaffen. Dat kan bij het doen van PIA's leiden tot langdurige onduidelijkheid, soms zelfs over kernvragen zoals wie nu precies de verantwoordelijke is voor een bepaalde verwerking.

Sommigen hebben er begrip voor dat toelichtingen bij de vragen van het Toetsmodel juridisch zijn gehouden opdat ze goed aansluiten bij de Wbp. Hoewel die insteek begrijpelijk is, lijkt het in de praktijk niet te leiden tot beter begrip. Een voorbeeld van verkeerd begrip is gegeven aan de hand van de noodzakelijkheidsvraag. Soms wordt deze vraag beantwoord met in gedachte de noodzakelijkheid van het project zelf, in plaats van dat aangetoond wordt dat de gegevensverwerking noodzakelijk is voor de doeleinden die met het project worden nagestreefd.

Sommige geïnterviewden zien heil in het verbeteren van de toelichting bij het Toetsmodel om dit soort problemen te lijf te gaan. Anderen geven aan dat de materie ook met duidelijke toelichtingen een uitdaging blijft, en dat het betrekken van privacydeskundigheid daarom onontbeerlijk is.

Stelling 3: de vragenlijst van het Toetsmodel is volledig

3 *(enigszins mee oneens)*

Er zijn een aantal elementen genoemd die nu in het Toetsmodel zouden ontbreken: gronden voor doorgifte naar landen buiten de EU, rechtvaardiging voor verdere verwerking bij het ontbreken van verenigbaarheid, toegang voor eenieder, bewerkersovereenkomst en meldingsplicht. Daarnaast is door personen gevraagd om aandacht in het Toetsmodel voor extra risico's bij ketens en/of koppelingen, big data, openbaarheid van gegevens en 'function creep' (het gebruik van gegevens bij projecten of wet- en regelgeving voor andere dan oorspronkelijke doeleneinden die niet verenigbaar zijn). Ook is aangegeven dat stakeholders, waaronder de betrokkenen zelf, unieke inzichten kunnen bieden op het gebied van privacygevolgen, maar dat handvatten hiervoor ontbreken in het Toetsmodel. Juist die handvatten zijn welkom volgens geïnterviewden omdat het effectief benaderen van deze groep een uitdaging is.

Naar aanleiding van de interviews hebben wij de indruk dat het voor sommigen niet zozeer het Toetsmodel zelf is dat onvolledig is, maar dat de geconstateerde onvolledigheid het resultaat is van de lastige vragen in het Toetsmodel. Niet alle uitvoerenden van een PIA weten de essentiële punten boven water te krijgen, ook al beantwoorden ze wel alle vragen. Vanuit ditzelfde inzicht ontbreken er volgens een aantal geïnterviewden uiteindelijk vaak drie essentiële aspecten: een goede risico-inschatting, het volledig in kaart brengen van het nut en de noodzaak van de gegevensverwerking en een proportionaliteitstoets. Door de personen die de PIA uitvoeren wordt dan ook aangegeven, dat ze het lastig vinden om risico's te benoemen.

Stelling 4: het Toetsmodel is een goed bruikbaar PIA-instrument

3 *(enigszins mee oneens)*

Stelling 5: het Toetsmodel is prettig om mee te werken

3 *(enigszins mee oneens)*

Opmerkingen over de gebruikersvriendelijkheid van het Toetsmodel zijn zaken als "onoverzichtelijk", "gedrocht" en "te veel tekst". Diverse malen worden de PIA-instrumenten van SURF en (in mindere mate) van NOREA hiertegenover gesteld als voorbeeld van hoe het beter kan. Verschillende geïnterviewden wezen op de voordelen van een digitale variant van een PIA-instrument, zoals SURF die standaard biedt en sommigen die zelf hebben ontwikkeld voor het PIA-instrument dat zij gebruiken. Geïnterviewden zagen bijvoorbeeld voordeel in het SURF-model omdat het in één oogopslag inzichtelijk maakt welke risico's er spelen bij een specifieke verwerking, en welke beveiligingsmaatregelen er nog genomen moeten worden. Een genoemd voordeel van het NOREA-model boven het Toetsmodel is het niet-juridische taalgebruik (maar wel met verwijzingen naar de wetgeving). Enkele geïnterviewden gaven aan dat ze het Toetsmodel gebruiken vanwege de verplichting daartoe, maar dit aanvullen met andere modellen. Zij karakteriseerden het Toetsmodel als niet gericht op uitvoeringsinstanties maar op beleidsmedewerkers en wetgevingsjuristen.

Stelling 6: Een light versie van het Toetsmodel zou goed zijn

3.5 *(tussen 'enigszins mee oneens' en 'enigszins mee eens')*

De scores op deze stelling liepen flink uiteen. Dat heeft er deels mee te maken dat een dergelijke "PIA-light"—of handvatten voor een verkorte vragenlijst—reeds is opgenomen in de toelichting bij het Toetsmodel. Deze versie van het Toetsmodel is echter bedoeld voor drie concrete situaties.[50] In de praktijk blijkt deze "PIA-Light" ook wel eens te worden gebruikt wanneer geen sprake is van zo'n situatie en eigenlijk dus het volledige Toetsmodel had moeten worden doorlopen. De gemiddelde score op deze vraag lag duidelijk hoger bij de geïnterviewden die ook daadwerkelijk het Toetsmodel gebruikt hebben.

Over alle stellingen in deze paragraaf heen waren de scores over het algemeen enigszins negatief, maar zoals aangegeven is er veelal sprake van een grote spreiding in de antwoorden. Die zit vooral tussen de geïnterviewden onderling: geïnterviewden waren in veel gevallen overwegend negatief, neutraal ofwel overwegend positief. In die verschillende groepen geïnterviewden zit geen duidelijke lijn, dat wil zeggen dat het niet zo is dat bijvoorbeeld alleen FG's of alleen beoordelaars van PIA's positief scoren.

Veel geïnterviewden hebben het belang benadrukt van zowel het duidelijk beschrijven van de verwerking als het maken van een belangenafweging als onderdeel van een PIA. De vragen die tijdens een PIA extra aandacht zouden moeten krijgen zijn: wat zijn de doeleinden van de verwerking, welke belangen zijn er in het spel, wat zijn de voorgenomen gegevensverwerkingen, en zijn die wel proportioneel (moeten de privacybelangen van personen niet zwaarder wegen dan wel de verwerking terughoudender ingericht worden)?

4 PIA-proces

De geïnterviewden kregen enkele stellingen inzake het PIA-proces voorgelegd. Hun werd verzocht om een cijfer toe te wijzen op dezelfde schaal als die in de vorige paragraaf.

Stelling 1: het is duidelijk wanneer een PIA moet worden uitgevoerd

4 *(enigszins mee eens)*

Enkele geïnterviewden gaven aan dat het duidelijk is wanneer een PIA moet worden uitgevoerd, simpelweg omdat het in de toelichting staat. Anderen gaven juist aan deze toelichting niet helder genoeg te vinden door het taalgebruik. Een deel van de laatstgenoemde groep heeft dat vervolgens zelf proberen op te lossen door medewerkers hier actief in te begeleiden.

Stelling 2: de rolverdeling tussen de bij de PIA betrokken personen is helder

4 *(enigszins mee eens)*

Slechts twee geïnterviewden scoorden hier negatief (één 1 en één 2). Niettemin gaven diverse geïnterviewden aan dat de rolverdeling bij het uitvoeren van een PIA duidelijker zou moeten zijn of duidelijker beschreven zou moeten worden in de toelichting.
Met name FG's geven aan dat hun rol voor anderen vaak onduidelijk is, waardoor zij bijvoorbeeld gezien worden als verantwoordelijke voor het uitvoeren van FG's, vraagbaak voor de werkvloer of "rijksbrede privacyadviseurs". Een niet-FG benadrukte het belang van onafhankelijke toetsing door de FG bij wetgevings-PIA's, omdat Kamerleden daarvoor te laat in het proces komen.

Stelling 3: het PIA-proces loopt in de praktijk goed

4 *(enigszins mee eens)*

Geïnterviewden zijn gemiddeld gezien gematigd positief over het PIA-proces. Het blijkt redelijk duidelijk te zijn wanneer en door wie een PIA uitgevoerd moet worden, en in de praktijk blijkt de uitvoering van het proces ook redelijk goed te lopen. Inzake de uitvoering van een PIA hebben een groot aantal geïnterviewden de toegevoegde waarde van workshops als onderdeel van het uitvoeren van een PIA benadrukt. Anderen gaven aan niets te zien in deze werkwijze, met name vanwege de tijdrovende exercitie, voorziene problemen in agendamogelijkheden en irrelevante discussies wanneer er te veel mensen aan tafel zitten. Het merendeel ziet workshops als een middel om tot een gezamenlijke visie te komen, vanuit verschillende rollen de inzichten te verzamelen en snel en efficiënt door de vragenlijst van het Toetsmodel heen te lopen. De snelheid werd dan verklaard door de aanwezigheid van een privacydeskundige die direct vragen van deelnemers kon beantwoorden. Een genoemd bijkomend voordeel van een PIA-workshop is dat deze bijdraagt aan het privacybewustzijn binnen de organisatie.

Het merendeel van de organisaties heeft wel enige vorm van beleid ten aanzien van het uitvoeren van PIA's, al houdt dat soms niet veel meer in dan dat men zich houdt aan het IAK. Enkele organisaties beschikken over volwaardig beleid en concrete processen. Dat er beleid is, wil overigens nog niet zeggen dat dat ook al 'geland' is in de organisatie, zo geven verschillende geïnterviewden aan.

De opdrachtgevers van de PIA's waarmee de geïnterviewden ervaring hebben blijken min of meer gelijkelijk verdeeld te zijn over de eerste lijn (denk hierbij bijvoorbeeld aan de verantwoordelijke directeur of de projectleider) en de tweede lijn (zoals de FG, de (wetgevings)jurist of de CIO).

Er blijkt een duidelijk patroon te zijn als het gaat om het betrekken van stakeholders[51] bij de uitvoering van een PIA: in de meeste gevallen worden er wel interne stakeholders betrokken die belangen hebben bij het project, maar niet de betrokkenen zelf of organisaties die hen vertegenwoordigen.

Voor zover zij daar zicht op hebben gaven de geïnterviewden aan dat in de helft van de PIA's de resultaten naar de CIO werden toegezonden, terwijl in driekwart van alle PIA's de resultaten werden toegezonden aan de FG. In veel gevallen werden de resultaten ook naar anderen toegezonden, hierbij ging het voornamelijk om de bij de PIA betrokken partijen (in de brede zin), de Autoriteit Persoonsgegevens en het parlement.

Tijdens de interviews zijn sommigen gevraagd naar hun visie inzake het openbaar maken van de uitkomsten van de PIA c.q. het (standaard) toezenden ervan aan het parlement. De responses hierop waren overwegend negatief. Argumenten hiervoor waren verschillend van insteek. Met betrekking tot het parlement werd aangegeven dat de Kamerleden niet de tijd en specialistische kennis bezitten om echt iets aan de PIA-rapporten te hebben; het toesturen van een volledig PIA-rapport kan dan in de praktijk juist minder effectief zijn dan het opnemen van een goede samenvatting in de Memorie van Toelichting. Ook de vraag naar het openbaar zijn in het algemeen werd met terughoudendheid beantwoord, bijvoorbeeld vanwege informatie die een risico zou vormen voor de veiligheid van systemen. Daarnaast is naar voren gebracht dat de wetenschap dat het rapport openbaar wordt de verantwoordelijke terughoudender zal maken bij het benoemen van heikele punten. Tegelijkertijd was er voor (gedeeltelijke) openbaarheid wel animo. Dit had enerzijds te maken met het creëren van bewustzijn in de organisatie zelf, anderzijds met het creëren van maatschappelijk draagvlak: een PIA-rapportage maakt inzichtelijk hoe er is nagedacht over de impact van gegevensverwerking op burgers en welke maatregelen er (kunnen) worden genomen om de negatieve impact zo klein mogelijk te laten zijn.

5 Verslaglegging

In ruim een derde van de gevallen bleef de verslaglegging over de PIA beperkt tot de ingevulde vragenlijst. In de overige gevallen werd een volledige PIA-rapportage opgeleverd, of werden de uitkomsten van de PIA verwerkt in bijvoorbeeld een beleids- of projectdocument.

Geïnterviewden kregen de vraag voorgelegd in welke mate specifieke elementen aanwezig waren bij de verslaglegging van (de resultaten van) de PIA. Hen werd gevraagd om een score toe te wijzen op de volgende schaal:

1. niet
2. beperkt
3. ruimschoots
4. volledig

Bij de analyse maken we onderscheid tussen het gebruik van het Toetsmodel (TPR) of van een alternatief model (ALT). De resultaten zijn weergegeven in onderstaande tabel.

	TPR	ALT
Beschrijving systemen en processen	2,5	3
Beschrijving persoonsgegevens	3	3
Juridische analyse	3	3,5
Overzicht privacyrisico's	2,5	3
Overzicht informatiebeveiligingsrisico's	2,5	2,5
Aanbevelingen voorkomen/mitigeren privacyrisico's	1,5	2
Aanbevelingen voorkomen/mitigeren inf. bev. risico's[52]	2	2

Vrijwel alle genoemde onderdelen blijken over het algemeen ten minste enigszins in rapportages aan de orde te komen. Rapportages op basis van alternatieve PIA-instrumenten zijn uitgebreider dan die op basis van het Toetsmodel, maar de verschillen zijn niet heel groot. Juridische analyses zijn zo goed als altijd aanwezig, terwijl aanbevelingen voor het voorkomen en het mitigeren van risico's daarentegen niet of beperkt aanwezig zijn.

6 Effect

De geïnterviewden kregen enkele stellingen voorgelegd inzake het effect van het uitvoeren van een PIA. Ze konden een cijfer kiezen van de eerder geïntroduceerde zespuntsschaal. De resultaten zijn weergegeven in onderstaande tabel.

	TPR	ALT
Hielp bij zicht krijgen op privacyrisico's	4,5	4
Had corrigerende/richtinggevende functie	4	3
Heeft geleid tot zorgvuldigere omgang met persoonsgegevens	4,5	3,5
Heeft bijgedragen aan draagvlak voor project	2,5	3

Verschillende geïnterviewden benadrukten het belang dat er wordt geborgd dat er ook daadwerkelijk iets gebeurt met de uitkomsten van de PIA. Daar is namelijk nog onvoldoende grip en zicht op. Het uitvoeren van een PIA kan desondanks een behoorlijk positieve invloed op de drie eerstgenoemde aspecten (zicht op risico's, corrigerende functie en zorgvuldigere omgang), al is dat zeker niet in alle gevallen zo. Het Toetsmodel blijkt hierop beter te scoren dan de alternatieve instrumenten. Dat is des te opvallender omdat er, zoals we hierboven zagen, bij het gebruik van alternatieve instrumenten uitvoeriger wordt gerapporteerd dan bij toepassing van het Toetsmodel. Opvallend is ook de hoge score op het punt "zicht krijgen op privacyrisico's" terwijl verschillende geïnterviewden aangeven dat aspect te missen in het Toetsmodel.

Het uitvoeren van een PIA blijkt slechts beperkt bij te dragen aan het draagvlak voor een project. Op dit punt scoort het Toetsmodel bovendien juist iets slechter dan alternatieve instrumenten. Dit verschil kan mogelijk worden verklaard door het gevoel dat soms aanwezig is bij de personen die het Toetsmodel moeten gebruiken. Er wordt gewaarschuwd dat het middel dit doel (een dialoog over privacy met daarbij ook de bewustwording) voorbij kan schieten. De kans daarop is groot op het moment dat het Toetsmodel wordt beleefd als een verplichte invuloefening. Op het moment dat personen daadwerkelijk inzien hoe een PIA kan bijdragen aan draagvlak voor een project of wetsvoorstel (of andersom beredeneerd, geen afbreuk kan doen daaraan) kan dit de uitvoering en bijbehorende effecten van het doen van een PIA ten goede komen.

Tot welke aanpassingen, aanvullingen, maatregelen enz. hebben de uitkomsten en/of aanbevelingen van de PIA geleid?

In enkele gevallen (waarbij het PIA's betrof op wetgeving) werden de onderliggende ontwikkelingen geheel of gedeeltelijk stopgezet dan wel significant inhoudelijk gewijzigd. Vaker bleef de essentie van het onderliggende project behouden (niet zelden vanwege wensen vanuit de politiek), maar werden er wel verbeteringen doorgevoerd in de gegevensverwerking of de waarborgen voor de rechtmatigheid, behoorlijkheid en zorgvuldigheid daarvan, zowel rechtstreeks (aanpassingen aan voorgenomen verwerkingen) als via wijzigingen in het wetsvoorstel. Ook heeft de PIA geholpen om aspecten van gegevensverwerking te onderbouwen, bijvoorbeeld in een Memorie van Toelichting. In brede zin werd regelmatig aangegeven dat het uitvoeren van een PIA een belangrijke bijdrage heeft geleverd aan een verhoogd privacybewustzijn bij de betrokken medewerkers.

47. Ook hadden sommige geïnterviewden nog andere rollen bij het PIA-proces, denk aan de adviseurs. De meeste genoemde overige rollen zijn echter redelijk in de drie in de tekst genoemde categorieën te passen.
48. De systeem-PIA's waren desondanks nog steeds substantieel in aantal.
49. Daarbij speelt mee dat personen in uitvoerende rollen vaak maar één keer te maken krijgen met een PIA.
50. De drie situaties genoemd in de Toelichting van het Toetsmodel:
    1. uitbreiding van het databestand binnen een bestaand ICT-systeem;
    2. gebruik van een bestaand databestand of ICT-systeem voor aanvullende of nieuwe doelen;
    3. koppeling van verschillende al bestaande databestanden of ICT-systemen voor bestaande of aanvullende of nieuwe doelen.
51. Zie Bijlage I in paragraaf 2.1.6 Consultatie van stakeholders.
52. Informatiebeveiligingsrisico's.

Format Interviewvragenlijst Evaluatie Toetsmodel PIA Rijksdienst

Onderzoekers: K. Versmissen, J. Terstegge, K. Siemers, W. Tran

In het interview zullen een aantal vragen gesteld worden over PIA's waarbij u zelf betrokken bent geweest. Het gaat dan over alle PIA's waarbij u zelf sinds 1 september 2013 betrokken bent geweest. Het maakt niet uit of bij die PIA's wel of niet van het Toetsmodel gebruik is gemaakt.

Algemene informatie

Uw naam:
Uw organisatie:
Uw afdeling:
Uw functie:
Uw telefoonnummer:
Uw e-mailadres:

Onderwerpen vragenlijst:

1. Uitvoeren PIA
2. Inhoud Toetsmodel
3. PIA-proces
4. Resultaat
5. Vervolgvragen

1. Uitvoeren PIA

1. Hoe vaak bent u sinds 1 september 2013 betrokken geweest bij een PIA?

2. Kunt u de onderliggende projecten noemen, in één zin beschrijven, en karakteriseren
   - ☐ wetgeving
   - ☐ beleid
   - ☐ systeemontwikkeling

3. Wat was uw rol bij deze PIA's?
   - ☐ opdrachtgever
   - ☐ uitvoerder
   - ☐ beoordelaar
   - ☐ anders

4. In welke fase van het project zijn de PIA's uitgevoerd?
   - ☐ pre-fase/voorafgaand
   - ☐ gedurende uitvoering project
   - ☐ tegen het einde van uitvoering project
   - ☐ na afronding/implementatie

5. Zijn de PIA's intern of extern uitgevoerd?
   - ☐ volledig intern
   - ☐ grotendeels intern
   - ☐ afwisselend
   - ☐ grotendeels extern
   - ☐ volledig extern

6. Hoeveel uur (in- en/of extern) is er per PIA besteed aan het uitvoeren daarvan?
   - ☐ < 10 uuur
   - ☐ 10–30 uuur
   - ☐ 30–100 uur
   - ☐ < 100 uur

7. Hoe groot was de rol van (in- en/of externe) privacydeskundigen bij het uitvoeren van de PIA?
   - ☐ < 10%
   - ☐ 10–30%
   - ☐ 30–80%
   - ☐ > 80%

8. Is bij alle projecten gebruik gemaakt van het Toetsmodel?
   ☐ Ja ☐ Nee. Zo nee,

8.a Waarvan dan wel, en hoe vaak?
   - ☐ NOREA, frequentie:
   - ☐ KING, frequentie:
   - ☐ intern opgesteld document, frequentie:
   - ☐ anders, frequentie:

8.b Wat waren de overwegingen om niet voor het Toetsmodel te kiezen?

Hanteer deze schaal voor het beantwoorden van onderstaande stellingen: 1–6:
1 volledig mee oneens
2 mee oneens
3 enigszins mee oneens
4 enigszins mee eens
5 eens
6 volledig mee eens

9. ☐ Het is duidelijk in welke gevallen er een PIA moet worden uitgevoerd

10. ☐ Het zou goed zijn als er ook een "light" versie van het Toetsmodel kwam

2. Inhoud Toetsmodel

11. ☐ De vragen van het Toetsmodel zijn op de praktijk toegesneden

12. ☐ De vragen van het Toetsmodel zijn begrijpelijk

13. ☐ De vragenlijst van het Toetsmodel is volledig

14. ☐ Het Toetsmodel is een goed bruikbaar instrument voor het uitvoeren van een PIA

15. ☐ Het Toetsmodel is prettig om mee te werken

3. PIA-proces

16. Heeft uw organisatie of organisatie-onderdeel beleid over het uitvoeren van PIA's en het toepassen van het Toetsmodel?
☐ Ja ☐ Nee

17. Wie gaf opdracht tot het uitvoeren van de PIA's waarbij u betrokken bent geweest?

18. Zijn bij het uitvoeren van de PIA's stakeholders betrokken?
☐ Ja ☐ Nee

19. Zijn de uitkomsten van de PIA's toegezonden aan de FG?
☐ Ja ☐ Nee

20. Zijn de uitkomsten van de PIA's toegezonden aan de CIO?
☐ Ja ☐ Nee

21. Zijn de uitkomsten van de PIA's toegezonden aan anderen, en zo ja, wie dan?
☐ Ja. Wie: ☐ Nee

Bij een PIA zijn verschillende personen betrokken, zoals beleidsambtenaren, wetgevingsjuristen, FG's, CIO's of systeemontwikkelaars. (Geef aan welk cijfer tussen 1–6 van toepassing is)

22. ☐ De rolverdeling tussen deze betrokkenen is helder

23. ☐ Het proces rondom het uitvoeren van PIA's en het toepassen van het Toetsmodel loopt in de praktijk goed

4. Resultaat

24. Hoe is verslag gelegd over de PIA's waarbij u betrokken bent geweest?
☐ Alleen lijst van antwoorden,
☐ PIA-rapportage,
☐ Anders, namelijk:

25. In hoeverre bevatte de verslaglegging de volgende elementen?

25a. ☐ een beschrijving van de belangrijkste systemen en processen
1 niet
2 beperkt
3 ruimschoots
4 volledig

25b. ☐ een beschrijving welke persoonsgegevens waar in deze systemen en processen verkregen, opgeslagen, verstrekt of anderszins verwerkt worden
1 niet
2 beperkt
3 ruimschoots
4 volledig

25c. ☐ een juridische analyse
1 niet
2 beperkt
3 ruimschoots
4 volledig

25d. ☐ een overzicht van privacyrisico's
1 niet
2 beperkt
3 ruimschoots
4 volledig

25e. ☐ een overzicht van informatiebeveiligingsrisico's
1 niet
2 beperkt
3 ruimschoots
4 volledig

25f. ☐ aanbevelingen voor het oplossen van gebleken juridische problemen
1 niet
2 beperkt
3 ruimschoots
4 volledig

25g. ☐ aanbevelingen voor het voorkomen of mitigeren van privacyrisico's
1 niet
2 beperkt
3 ruimschoots
4 volledig

25h. ☐ aanbevelingen voor het voorkomen of mitigeren van informatiebeveiligingsrisico's
1 niet
2 beperkt
3 ruimschoots
4 volledig

26. Tot welke aanpassingen, aanvullingen, maatregelen enz. hebben de uitkomsten en/of aanbevelingen van de PIA's geleid (op hoofdlijnen)? (Belangrijke vraag, m.a.w.: Wat is er nou echt veranderd of bijgesteld n.a.v. de PIA?)

Geef een cijfer 1–6 voor de mate waarmee u het eens bent met de volgende stellingen.

27. ☐ Toepassing van het Toetsmodel heeft geholpen om zicht te krijgen op de privacyrisico's

28. ☐ Toepassing van het Toetsmodel heeft een richtinggevende of corrigerende functie gehad

29. ☐ Toepassing van het Toetsmodel heeft geleid tot een zorgvuldigere omgang met persoonsgegevens

30. ☐ Toepassing van het Toetsmodel heeft bijgedragen aan het draagvlak voor het project

5. Vervolgvragen

N.B. Deze vervolgvragen zijn bedoeld voor het tweede, opener gedeelte van het interview.

31. Openingsvraag: Heeft u op basis van uw ervaringen suggesties voor hoe het PIA-proces en het Toetsmodel verbeterd kunnen worden?

32. Doorvragen over opinies met opvallend lage/negatieve score: wat is er dan precies mis, en hoe kan het beter?

33. Afsluitende vraag: Is er verder nog iets wat u kwijt wilt over PIA's en het Toetsmodel?

34. Extra: Zijn er personen binnen of buiten uw organisatie waarvan u denkt dat het goed is als we zijn of haar expertise betrekken in het onderzoek?

Bijlage III – Enquête

Aansluitend op de mondelinge interviews is er een online enquête uitgezet.[53] Hierin konden respondenten hun ervaringen kwijt met standpunten over en suggesties voor het Toetsmodel PIA Rijksdienst of het PIA-proces. Hiernaast bood de enquête ons de mogelijkheid om diverse stellingen en standpunten te kwantificeren en te vergelijken met de resultaten uit de mondelinge interviews.

In dit hoofdstuk beschrijven we de uitkomst van de enquête. De kwantitatieve gegevens dienen met enige terughoudendheid beschouwd dienen te worden, zowel vanwege de relatief beperkte groep van respondenten als vanwege de soms grote spreiding van antwoorden. Dankzij de aan respondenten geboden mogelijkheid om toelichtingen te geven bij ieder antwoord hebben wij de kwantitatieve uitkomsten van de enquête wel kunnen aanvullen met kwalitatieve gegevens.

Achtereenvolgens komen de volgende aspecten aan de orde:
- De wijze waarop de geïnterviewden bij PIA's betrokken zijn geweest
- Het uitvoeren van een PIA
- De inhoud van het Toetsmodel
- Het PIA-proces
- Verslaglegging over de PIA, en
- Het effect van de PIA

1 Betrokkenheid respondent bij PIA's

Alle respondenten zijn (of waren na 1 september 2013) werkzaam bij de Rijksoverheid. Dit was een voorwaarde voor deelname aan de enquête. Bijna de helft van de respondenten is in een uitvoerende rol betrokken geweest bij het uitvoeren van een PIA, al dan niet op basis van het Toetsmodel. Veel minder vaak hadden respondenten een opdrachtgevende of toezichthoudende functie rol (resp. 16% en 14%). Een derde van de respondenten viel in de restcategorie. Rollen die hierbij zijn ingevuld zijn onder andere (juridisch) adviseur, lid van Medezeggenschapsraad of Ondernemingsraad, projectontwikkelaar, stakeholder, inkoopadviseur, programmamanager.

Zes op de tien de respondenten zijn betrokken geweest bij 1 of 2 PIA's, een op de drie bij 3 tot 5 PIA's. Een enkele respondent heeft aangegeven nooit betrokken te zijn geweest bij een PIA. Tot slot heeft 8% aangegeven betrokken te zijn geweest bij 5 of meer PIA's.

2 Uitvoering PIA

PIA-proces in goede banen leiden
Respondenten kregen de vraag wat de beste manier zou zijn om een PIA-proces in goede banen te leiden.[54] De antwoorden waren als volgt:

Een losse toelichting bij het PIA-instrument die het PIA-proces beschrijft	*33%*
Een vragenlijst die de uitvoerder 'automatisch' door het PIA-proces leidt	*60%*
Elke instantie mag haar eigen PIA-methodiek ontwikkelen	*8%*

Een respondent geeft als visie dat afhankelijk van aanleiding, doel en context alle drie bovengenoemde opties mogelijk moeten zijn om de PIA in goede banen te leiden. Het merendeel van de respondenten geeft de voorkeur aan een PIA-instrument in de vorm van een vragenlijst die de uitvoerder 'automatisch' door het PIA-proces leidt. Dit wordt onder meer toegelicht door vergelijkingen te maken met het Tactisch normenkader van de BIR. Een 'meetlat' in het PIA-instrument zou kunnen helpen, maar bovenal wordt aangegeven dat vragen logisch moeten zijn, elkaar dienen op te volgen en (meer) toelichting beschikbaar moet zijn. Een respondent benadrukt het belang van privacybewustzijn en geeft aan dat een PIA-vragenlijst niet slechts een invuloefening moet zijn. Dit past bij de visie van een ander dat het instrument zelf van marginale invloed is en het vooral aan de manier van oppakken door directie ligt en de personen die daarbij betrokken zijn.

Behoefte aan uitvoeringscriteria

Respondenten kregen een vraag voorgelegd om hun behoefte te peilen voor duidelijke criteria ter uitvoering van een PIA.[55] Een klein deel heeft aangegeven dat de huidige handreikingen voldoende duidelijk zijn om een PIA uit te voeren. Zes van de tien respondenten zouden echter graag duidelijke criteria in de vorm van een pre-scan zien, terwijl meer dan vier van de tien de voorkeur geven aan uitvoeringscriteria in de vorm van een handleiding. Eén van de respondenten merkt hierbij op dat het duidelijk (begrijpelijk) moet zijn voor de beleidsmedewerkers/'leken'/niet-juristen en dat dit in de huidige situatie nog niet altijd zo is.

3 Inhoud Toetsmodel

Respondenten kregen in de enquête diverse stellingen voorgelegd die ook in de mondelinge interviews aan bod zijn gekomen. Alleen respondenten die aangaven dat zij PIA's aan de hand van het Toetsmodel hebben uitgevoerd konden deze vragen beantwoorden. Dat was bijna driekwart van het totaal. Aan hen is gevraagd om een cijfer toe te wijzen conform de volgende schaal:[56]

1. volledig mee oneens
2. mee oneens
3. enigszins mee oneens
4. enigszins mee eens
5. eens
6. volledig mee eens

Wanneer wij hieronder aangeven dat respondenten het eens of oneens waren met een stelling, dan hebben zij respectievelijk een van de eerste drie antwoorden (enigszins tot volledig mee eens) of een van de laatste drie antwoorden (enigszins tot volledig mee oneens) gegeven.

Stelling 1: de vragen van het Toetsmodel zijn op de praktijk toegesneden

De stelling is redelijk positief beantwoord: de royale helft van de respondenten is het eens met de stelling, tegenover iets minder dan vier op de tien die het ermee oneens zijn. Een enkele respondent heeft hierbij opgemerkt dat de praktijk er baat bij zou hebben als de vragenlijst en de Toelichting van het Toetsmodel een minder juridische insteek hadden. Ook werd opgemerkt dat de vragenlijst meer leidt tot een bevestiging van de situatie. Volgens andere toelichtingen biedt het Toetsmodel te weinig concrete handvatten om beveiligingsmaatregelen te bepalen.

Stelling 2: de vragen van het Toetsmodel zijn begrijpelijk

Ook deze stelling is vrij positief beantwoord: bijna twee derde van de respondenten heeft gesteld het ermee eens te zijn dat de vragen van het Toetsmodel begrijpelijk zijn, tegenover ruim een derde dat het er mee oneens is. De respondenten merken op dat de begrijpelijkheid van het Toetsmodel erop vooruit zou gaan als de vragenlijst en de

Toelichting meer praktisch worden ingestoken (in plaats van juridisch). Een respondent met een juridische achtergrond heeft opgemerkt dat het Toetsmodel voor hem of haar zelf wel begrijpelijk is maar dat het voor collega's een lastig document blijkt.

Stelling 3: de vragenlijst van het Toetsmodel is volledig

Als het gaat over de volledigheid van de vragenlijst van het Toetsmodel overheerst een positief geluid. Ruim de helft van de respondenten is het eens met de stelling, tegenover minder dan een derde dat het er mee oneens is.

Maar liefst een kwart van de respondenten heeft echter opgemerkt dat ze deze stelling niet konden beoordelen omdat ze de kennis hiervoor misten of het Toetsmodel niet op zijn volledigheid hebben getoetst. Ook werd aangegeven dat het Toetsmodel juist overcompleet is; dit rijmt met toelichtingen waarin wordt aangegeven dat de lijst erg uitgebreid is. Respondenten noemen verder dat het Toetsmodel een grondslagtoetsing voor elke verwerking, vragen over (sub)bewerkers en concrete handvatten voor een eigenaar van een verwerking ontbeert. Tot slot is ook nog opgemerkt dat het nodig is dat de gebruiker de juiste scope voor ogen heeft bij de beantwoording van de vragen om volledige resultaten te krijgen.

Stelling 4: het Toetsmodel is een goed instrument om privacyrisico's in kaart te brengen

Bij deze stelling is opnieuw een gematigd positieve beoordeling gegeven. Zes op de tien geven aan dat ze het eens zijn met de stelling, tegenover een derde dat heeft aangegeven het er mee oneens te zijn.

Toelichtingen geven aan dat de PIA helpt om de beleidsafdeling te dwingen na te denken over de concrete werking en over bijbehorende zaken die moeten worden geregeld. Aan de andere kant wordt ook genoemd dat het Toetsmodel wel nog verder moet worden ontwikkeld. Om risico's daadwerkelijk goed in beeld te brengen dient hiervoor een risicoanalyse te worden uitgevoerd.

Stelling 5: het Toetsmodel is prettig om mee te werken

Op deze stelling reageren de respondenten verdeeld. De helft is het er mee eens, de andere helft mee oneens. Enkele respondenten geven aan dat ze het Toetsmodel te veel toegespitst vinden op bestaande situaties. Sommige vragen leiden wel tot nadenken maar zouden extra verduidelijkt moeten worden, bijvoorbeeld door middel van concrete voorbeelden.

Stelling 6: de light versies zijn een zinvolle uitbreiding van het Toetsmodel

Bijna een derde van de respondenten blijkt onbekend te zijn met de light versie van het Toetsmodel. Degenen die de light versie wel kennen, antwoorden overwegend positief op deze stelling: ruim twee derde is het er mee eens, tegenover iets minder dan een derde dat het er mee oneens is.

Een enkele respondent merkt op dat een light versie de gebruikersvriendelijkheid kan verhogen. Ook wordt meermaals aangegeven dat er vaak toch wordt gevraagd om een volledige PIA.

Beste vorm voor een PIA-instrument (a)[57]

Respondenten zijn verdeeld op dit punt. Ruim vier op de tien geven de voorkeur aan een integraal instrument, vier op de tien zien liever gescheiden instrumenten: één gericht op beleid en wetgeving en het andere op processen en systemen. Laatstgenoemde groep heeft haar standpunt onderbouwd met het argument dat ICT-personeel vastloopt op de juridische aspecten van de gegevensverwerking. Maar ook wordt genoemd dat de PIA in zijn huidige vorm meer tot een juridische 'tool' is geworden waarbij teveel mensen een rol wensen te spelen. Respondenten hebben toegelicht dat ook bij een splitsing in twee instrumenten de beoordeling uiteindelijk alsnog maatwerk vergt. Ook werd aangegeven dat één integraal document juist de samenhang bewaakt. Daarnaast werden andere opties gegeven, zoals een online module

op basis van business rules, het toevoegen van een risicoanalyse of een niet nader omschreven vorm die hoe dan ook verder gaat dan alleen de vragenlijst (vanwege de situatie dat het Toetsmodel nu te weinig zegt over risico's en de impact op betrokken partijen).

Beste vorm voor een PIA-instrument (b)[58]
Respondenten kregen ook de mogelijkheid om aan te geven of ze de voorkeur geven aan een PIA-instrument in de huidige vorm (een vaste lijst vragen) of liever een kader krijgen met randvoorwaarden waarvan de invulling verder vrij is. Hier bleek een vrij duidelijke voorkeur voor een vaste vragenlijst (vier op de tien) boven een kader met randvoorwaarden (ruim twee op de tien). Een derde geeft aan beide opties graag gecombineerd te zien.

Argumenten voor een vaste vragenlijst waren onder andere om de nodige richting te geven en om de uniformiteit (o.a. in risicoclassificatie en beveiligingsmaatregelen) te waarborgen. Als argument voor een rand¬voorwaardelijk kader is aangedragen dat de PIA moet leiden tot inzicht door middel van een open discussie, en dat een strikte vragenlijst daarvoor niet handig is. Ook degenen die graag een combinatie van beide mogelijkheden zien geven aan dat het instrument het gesprek tussen privacy officers, opdrachtgever en uitvoerder dient te stimuleren of faciliteren. Het moet mogelijk blijven maatwerk te leveren, en een vaste vragenlijst zou niet meerdere vragen per onderdeel moeten stellen. Ook hier wordt de link gelegd met het analyseren en classificeren van risico's en de daaruit voortvloeiende maatregelen.

4 PIA-proces

In de enquête kregen respondenten enkele stellingen inzake het PIA-proces voorgelegd. Hun werd gevraagd om een cijfer toe te wijzen op dezelfde schaal als die in de vorige paragraaf. Ook hier konden respondenten, indien gewenst, een nadere toelichting opgeven.

Stelling 7: PIA's worden soms niet uitgevoerd omdat degene die ervoor verantwoordelijk is niet weet dat een PIA verplicht is
Maar liefst ruim 85% van de respondenten is het eens met deze stelling. Het merendeel van hen heeft de score 5 ("mee eens") gegeven. Een enkele respondent merkt hierbij op dat de PIA onderdeel uitmaakt van de IAK en dat het om deze reden juist wel helder is wanneer een PIA uitgevoerd moet worden. Een andere respondent geeft aan dat iedereen wel weet heeft van de PIA-verplichting, maar dat het PIA-proces soms wel eerder in gang gezet dient te worden. Ook wordt aangegeven dat het niet uitvoeren van een PIA soms het gevolg is van het ontbreken van een privacy officer die toezicht uitoefent en weet wat er speelt.

Stelling 8: de rolverdeling tussen de bij de PIA betrokken personen is helder
De reacties op deze stelling vertonen een opmerkelijk patroon. Niet één respondent geeft aan het volledig eens of oneens te zijn met de stelling, maar degenen die "mee eens" of "mee oneens" antwoorden (drie resp. vier op de tien respondenten) zijn groter in aantal dan zij die "enigszins mee eens" of "enigszins mee oneens" antwoorden (één resp. twee op de tien). Kennelijk hebben veel respondenten hier een duidelijk beeld bij, zonder dat dat extreme vormen aanneemt. De teneur is negatief.

Als notitie heeft een enkele respondent opgemerkt dat de rolverdeling het liefst nog duidelijker mag worden opgeschreven. Een ander aandachtspunt is volgens respondenten dat het (in de praktijk) niet duidelijk is dat de PIA ook bij de FG moet worden gemeld en relevant is voor de CIO.

Stelling 9: het PIA-proces loopt in de praktijk goed

Het gemiddelde antwoord op deze stelling is gematigd negatief. Ruim de helft van de respondenten vindt dat het PIA-proces in de praktijk (enigszins) niet goed verloopt, tegen vier op de tien die de stelling (enigszins) positief beantwoorden.

Hierbij is opgemerkt dat vragen uit het Toetsmodel (te) gemakkelijk afgedaan kunnen worden door 'niet van toepassing' aan te geven. Daarnaast is aangegeven dat het PIA-proces iteratiever zou mogen zijn, zonder afbreuk te doen aan het moment van toetsing. Dit sluit aan bij de opvatting dat er op dit moment wel veel diversiteit bestaat in benadering, proces, inhoud en moment van inzet. Over laatstgenoemde wordt gezegd dat de start van het PIA-proces soms tijdiger zou kunnen. Over het algemeen kan gezegd worden dat respondenten de verloop van het PIA-proces matig vinden.

Betrekken van (vertegenwoordigers van) betrokkenen

Respondenten is gevraagd om na te denken over de mate waarin zij denken te kunnen voldoen aan de toekomstige verplichting, voortvloeiend uit de Europese AVG, om 'waar passend' de personen van wie persoonsgegevens worden verwerkt (of organisaties die hen vertegenwoordigen) te consulteren bij de uitvoering van een PIA[59]. Ruim een derde heeft aangegeven aan deze verplichting te kunnen voldoen en ook te weten welke organisaties daarvoor te moeten benaderen. Van de overige respondenten weten ruim twee op de tien niet welke betrokkenen ze kunnen consulteren en vinden bijna twee op de tien consultatie onwenselijk.

Meerdere respondenten hebben kanttekeningen geplaatst bij het consulteren van betrokkenen. Zo zal de werkbaarheid daarvan sterk afhangen van het onderliggende project (vooral als het gaat om PIA's voor beleid). Eveneens aangegeven is dat een respondent wel weet wie hij moet consulteren, maar niet hoe hij of zij dit kan organiseren. In samenhang met laatstgenoemde wordt ook aangegeven dan niet alle betrokkenen goed georganiseerd zijn of voldoende menskracht hebben. Een andere respondent merkt op dat het niet wenselijk is alle betrokkenen te consulteren en daarna achteraf niet aan bepaalde 'verwachtingen' te kunnen voldoen. Aansluitend is opgemerkt dat hiervoor de medezeggenschap betrokken kan worden en dat maatschappelijke belangenorganisaties een goede rol kunnen spelen. Echter wordt het betrekken van vertegenwoordigende organisaties ook door enkelen juist gezien als risico op (bewuste) vertraging en belemmering vanuit deze organisaties. Ook wordt de consultatie op zichzelf al gezien als een tijdrovende klus. Een van de respondenten geeft aan dat consultatie de verantwoordelijkheid van 'het beleid' is.

Personen te betrekken in workshop

Aan respondenten is gevraagd om aan te geven wie zij minstens aanwezig willen zien bij een workshop ter uitvoering van een PIA voor beleid of wetgeving.[60] De volgorde van meest naar minst gekozen rollen is als volgt:

- een Wbp-coördinator/de privacydeskundige
- de betrokken beleidsmedewerkers
- een (wetgevings)jurist
- de CIO/iemand van de CIO-office
- (gedeelde plaats)
  - betrokken (project)medewerkers
  - betrokken ketenpartner(s)
- een procesbegeleider
- de FG

Diezelfde vraag is gesteld inzake een workshop ter uitvoering van een PIA op processen of systemen.[61] De volgorde van meest naar minst gekozen rollen is dan als volgt:

- (gedeelde plaats)
  - een informatiebeveiligingsexpert
  - een Wbp- coördinator/de privacydeskundige
- vertegenwoordigers van de gebruiker(s) van het systeem
- betrokken (project)medewerkers

- betrokken ketenpartner(s)
- eventuele bewerkers
- (gedeelde plaats)
- de CIO/ iemand van het CIO-office
- betrokken beleidsmedewerkers
  - de FG
  - een procesbegeleider

De toelichtingen bij de bovenstaande twee vragen gaan vrijwel gelijk op. Respondenten zijn het over het algemeen met elkaar eens dat dat de groep niet te groot mag zijn ter bevordering van de efficiëntie. Ook hangt de selectie van personen waarvan de aanwezigheid gewenst is af van het moment en de aard en grootte van het onderliggende project. Tegelijkertijd is ook door één persoon genoemd dat een PIA voor iedereen intern relevant is, gelet op het belang van het creëren van een gezamenlijke visie.

De rol van de FG en CIO wordt wel gezien als optioneel (alleen wanneer het aan de orde of relevant is) dan wel voorafgaand aan of volgend op een PIA-workshop.
Ook is geopperd om aan de voorkant een soort snelle stakeholderanalyse te doen, zodat ingeschat kan worden welke selectie van aanwezigen het handigst is.

Tot slot is voor PIA-workshops met het oog op beleid of wetgeving ook gesuggereerd dat externe stakeholders die betrokkenen vertegenwoordigen daarin een rol zouden kunnen krijgen. Voor de workshops met het oog op processen of systemen is door respondenten een proceseigenaar/lijnmanager (degene die het in praktijk moet gaan doen) genoemd en een auditor.

Verbetering omgang met privacyrisico's binnen de Rijksoverheid
Respondenten konden punten verdelen over vijf opties voor het verbeteren van de manier waarop er binnen de Rijksoverheid wordt omgegaan met de privacyrisico's van nieuw beleid of wetgeving, of van nieuwe systemen of processen.[62] Dit leidde tot onderstaande ranglijst.
1. beschikbaar stellen van een interactief digitaal PIA-instrument (28%)
2. aanbieden van een pool van PIA-experts die kunnen worden ingeschakeld bij uitvoering (23%)
3. aanbieden van PIA-trainingen (19%)
4. aanbieden van een helpdesk voor vragen en begeleiding (17%)
5. aanbieden van benchmarks voor de kwaliteit van PIA's (10%)

5 Verslaglegging

Respondenten kregen de vraag voorgelegd in welke mate specifieke elementen aanwezig waren bij de verslaglegging van (de resultaten van) de PIA uitgevoerd op basis van het Toetsmodel.[63] Hen werd gevraagd om een score toe te wijzen. De responses vertonen geen grote afwijkingen in vergelijking met de uitkomsten uit de mondelinge interviews. Van vrijwel alle genoemde onderdelen wordt ook hier aangegeven dat ze ten minste 'beperkt' in rapportages aan de orde komen. Een beschrijving van persoonsgegevens blijkt in verhouding het vaakst in zijn volledigheid in rapportages opgenomen te worden. Opvallend is dat de respondenten op de enquêtes positiever antwoorden met betrekking tot de aanbevelingen voor het voorkomen of mitigeren van privacyrisico's. Waar deze nagenoeg ontbreken in de rapportages volgend uit de mondelinge interviews hebben respondenten bij de enquête aangegeven dat deze aanbevelingen eerder beperkt en ruimschoots aanwezig zijn in de rapportages dan ontbreken.

Hieronder de resultaten:[64]

	TPR
Beschrijving systemen en processen	2,5
Beschrijving persoonsgegevens	3
Juridische analyse	2,25 ▼
Overzicht privacyrisico's	2,5
Overzicht informatiebeveiligingsrisico's	2,25 ▼
Aanbevelingen voorkomen/mitigeren privacyrisico's	2,25 ▲
Aanbevelingen voorkomen/mitigeren inf. bev. risico's	2

64. Gemiddelde respons per verslagleggingsaspect.
Schaal: 1 = niet, 2 = beperkt, 3 = ruimschoots, 4 = volledig.
De cijfers met een ▼ wijken af naar beneden in vergelijking met de mondelinge interviews.
De cijfers met een ▲ wijken af naar boven in vergelijking met de mondelinge interviews.

Beschikbaarheid/openbaarheid definitieve PIA-resultaten

Respondenten werden gevraagd voor wie de definitieve resultaten van een uitgevoerde PIA beschikbaar zouden moeten zijn.[66] Er blijkt een vrij overtuigende voorkeur voor het redelijk breed verspreiden van de definitieve resultaten. Ruim een derde wil de resultaten voor iedereen toegankelijk (openbaar) maken. Toelichtingen bij dit antwoord geven wel aan dat bepaalde onopgeloste technische problemen of veiligheidsmaatregelen dienen te worden uitgezonderd van openbaarheid. Iets minder dan de helft van de respondenten (44%) wil het resultaat verspreiden onder het (project)team, het MT, de politieke leiding en andere betrokken departementen c.q. Rijksdiensten. Argumenten hiervoor zijn inzicht in risico's, verantwoordelijkheid bij de juiste personen en kennisdeling. Genoemd wordt ook dat het soms belangrijk kan zijn het rapport in de eigen organisatie breed te publiceren.

6 Effect

Respondenten kregen enkele stellingen voorgelegd inzake het effect van het uitvoeren van een PIA. Ze kenden een cijfer toe op de reeds geïntroduceerde zespuntenschaal. Ook hier hebben respondenten de mogelijkheid gekregen om hun antwoord toe te lichten.

Stelling 10: de uitvoering van een PIA heeft geholpen bij het zicht krijgen op privacyrisico's

Respondenten hebben deze stelling positief beoordeeld: meer dan driekwart is het ermee eens. Een respondent maakt daarbij wel als kanttekening dat het verkregen resultaat in zijn of haar geval niet was toe te rekenen aan het Toetsmodel. Een ander geeft aan dat met name de combinatie met een (aparte) risicoanalyse het resultaat kwalitatief verbeterde.

Stelling 11: de uitvoering van een PIA had een corrigerende c.q. richtinggevende functie

Ook deze stelling is door respondenten positief beoordeeld. Ruim zeven op de tien geven aan dat het uitvoeren van een PIA een corrigerende of richtinggevende functie heeft gehad. Door een respondent die het oneens was met de stelling wordt aangegeven dat de PIA doorgaans wordt gezien als 'een verplicht hoepeltje'.

Stelling 12: de uitvoering van een PIA heeft geleid tot een meer zorgvuldige omgang met persoonsgegevens

In het verlengde van stelling 11 geeft driekwart van de respondenten bij deze stelling aan dat ze het eens zijn met dat de uitspraak dat de uitvoering van een PIA heeft geleid tot een meer zorgvuldige omgang met persoonsgegevens. Opmerkingen hierbij geplaatst geven aan dat er dankzij de PIA in ieder geval beter over wordt nagedacht, en dat er sowieso al zorgvuldig met persoonsgegevens wordt omgegaan wanneer men zich bewust is van de risico's.

Stelling 13: de uitvoering van een PIA heeft bijgedragen aan het vergroten van het draagvlak van het project

Iets meer respondenten zijn het eens met deze stelling (46%) dan er respondenten zijn die het ermee oneens zijn (43%). Toelichtingen verduidelijken dat discussies naar aanleiding van een PIA niet altijd hartelijk worden ontvangen. Daarnaast wordt aangegeven dat een PIA draagvlak kan creëren bij juristen een draagvlak en in ieder geval wel bijdraagt aan de kwaliteit van het onderliggende project.

Effecten toepassing Toetsmodel PIA Rijksdienst

In de enquête is ook een vraag opgenomen over de *feitelijke* effecten de toepassing van het Toetsmodel teweeg heeft gebracht.[67] Dit leverde de volgende ranglijst op:

- groter privacybewustzijn in de organisatie
- inzicht in de details van de verwerkingen van persoonsgegevens
- meer inzicht in de privacyrisico's van het beleid en of de verwerking,
- meer inzicht in de informatiebeveiligingsrisico's
- overeenstemming over de benodigde waarborgen
- tijdige bijsturing of stopzetten van het project

In de categorie "anders en/of toelichting" werden ook nog genoemd 'stress' en 'een hoop gedoe zonder dat het beoogde resultaat (borging, inzicht) prevaleert'.

(Gewenste) Effecten toepassing PIA-instrument

Aansluitend op de vorige vraag werd respondenten gevraagd naar de gewenste effecten van het toepassen van een PIA-instrument.[68] Dit leverde de volgende ranglijst op:

- groter privacybewustzijn in de organisatie
- meer inzicht in de privacyrisico's van het beleid en of de verwerking
- inzicht in de details van de verwerkingen van persoonsgegevens,
- meer inzicht in de informatiebeveiligingsrisico's
- overeenstemming over de benodigde waarborgen
- tijdige bijsturing of stopzetten van het project

In de categorie "anders en/of toelichting" is ook 'vertrouwen' nog genoemd als gewenst effect.

7 Open slotopmerkingen

De respondenten is aan het einde van de vragenlijst de mogelijkheid geboden om aan te geven wat zij verder nog kwijt wilden over PIA's bij de Rijksoverheid en/of het Toetsmodel. Onderstaand overzicht bevat de opmerkingen die respondenten in het open tekstveld hebben gegeven met betrekking tot het Toetsmodel of PIA's in het algemeen. We hebben deze gegroepeerd op proces en inhoud.

Inhoud

- De vragen zouden minder juridisch geformuleerd moeten worden. Voor een niet-jurist is het geen prettige taal.
- Sommige vragen horen aan het begin (de waarom vragen), sommige aan het einde (de hoe ga je het precies inrichten vragen).
- De PIA is veel te technisch voor beleidsmedewerkers.
- Als een PIA niet het hele proces meeneemt, kunnen er risico's blijven liggen. Risico's die voor de gehele rijksdienst gelden! Je kunt dus een mooi instrument hebben maar er is meer nodig!
- Ik mis v.w.b. PIA's bij systemen een veel duidelijkere connectie met beleid en normenkaders (de baseline informatiebeveiliging Rijksdienst). De Rijksoverheid moet afstappen van haar keuze om de AV23 (Achtergrondstudies en Verkenningen nummer 23 te blijven gebruiken.
- Het huidige Toetsmodel richt zich te zeer op de juridische invalshoek van bescherming van persoonsgegevens. In een nieuw model zouden de organisatorische en technologische invalshoek een prominentere rol moeten gaan spelen.
- Voorkomen moet worden dat een PIA naar het voorkeursalternatief wordt toegeschreven.
- Gegevensminimalisatie is nog taboe.
- Het kan een zeer goed instrument zijn als het verder wordt ontwikkeld en ook maatregelen kan genereren. Maar wellicht niet te ingekaderd omdat dan gemakzucht de overhand neemt en dus schijn inzicht in risico's.
- Met een PIA alleen ben je er niet en voldoe je nog niet aan de Wbp. Maak de PIA dus WBP proof door een format voor het uitvoeren van een risicoanalyse toe te voegen aan de vragenlijst welke voldoet aan de door de Wbp gestelde eisen aan zo'n analyse.
- Bij de 3 PIA's waarbij ik betrokken was constateerde ik een duidelijke overlap met de Quickscan BIR. Deze 2 stromen bestaan binnen VenJ naast elkaar waardoor er dubbelingen ontstaan in het beantwoorden van vragen. Graag integreren met elkaar.

Proces

- Soms kan de PIA ook in omgekeerde volgorde gebruikt worden, om wetgeving aan te passen aan een reeds bestaande praktijk, als voor die praktijk (het uitwisselen van BSN-nummers) nog geen wettelijke basis bestond.
- Praktijk is dat de PIA Rijksoverheid op dit moment aan het verworden is tot een invullijstje wat beleefd wordt als een moetje.
- De PIA is op papier verplicht, zou dwingender moeten worden voorgeschreven— zonder PIA kan een initiatief of project niet naar een volgende fase.
- In het proces van een PIA is de ervaring dat een uitgevoerde PIA als oneigenlijk aspect is gebruikt door stakeholders voor andere belangen (bijv datgene behouden dat er is).
- De huidige privacy-verantwoordelijke wordt meestal door de bestuurder benoemd en kan in die hoedanigheid niet altijd een onafhankelijke positie innemen. Het is daarom wenselijk om rijksbreed een aparte pool van PIA-verantwoordelijken te hebben.
- Betrek vooral ook de medezeggenschap tijdig. En promoot Privacy by design ipv PIA achteraf.
- Het opstellen van een PIA is nu toch vooral een verplicht nummer waarvan onduidelijk is hoe dit in het beleidsproces is ingebed.
- Een PIA wordt volgens mij veelal in een laat stadium verricht, als beleid of wetgeving al in vergaand stadium is gevormd. Het is volgens mij soms lastig om het juiste moment te bepalen, maar het ligt vaak vroeger in het proces dan gedacht.

- Het PIA-proces wordt m.i. teveel als 'lineair' proces aangevlogen i.p.v. als een interactieve manier om op een gestructureerde manier in gesprek te komen over de maatregelen die getroffen moeten worden. Daarbij is het toetsmoment niet altijd helder.
- Ik vind het heel goed dat er een dergelijk model is, het is een stok achter de deur, dwingt beleid tot nadenken, ook belangrijk in huidige digitale tijd met grote informatiestromen waarmee privacybescherming op gespannen voet staat PIA-proces en rapportage is vaak erg omvangrijk (soms 100+).
- Dure bureaus/externen die het doen. Uitkomsten soms willekeurig en erg divers. Hierdoor zijn inzichten uit verschillende PIA's slecht vergelijkbaar, soms zelfs tegenstrijdig.
- De PIA wordt gezien als instrument dat je in 1x invult. Dit past niet.
- Het zou fijn zijn als het Toetsmodel PIA Rijksdienst (deze of nieuwere versie) voorgeschreven werd als instrument. Nu zijn er te veel PIA-varianten.
- Ook PIA is continu PDCA + bewustwording op hoger planniveau.
- Met uitvoering door externe partij geen goede ervaring opgedaan omdat deze partij zich te veel als wetgevingsjurist en beslisser zag.
- Mooie resultaten zijn al bereikt, doorpakken en vasthouden maar zeker ook door ontwikkelen en integraliteit nastreven/borgen.
- De wetenschap dat er een PIA bestaat en de noodzaak tot invullen zijn in brede zin steeds meer bekend. Wij hebben als afdeling Juridische zaken een goede lijn naar onze directie Informatievoorziening (die gaan over de systemen) en bij alle nieuwe ontwikkelingen terzake wordt een PIA opgesteld.
- In het kader van de Wet Meldplicht Datalekken gaan we in dat verband projectmatig ook een inhaalslag doen naar alle lopende systemen. Wat dat betreft heeft wellicht niet zozeer de PIA alswel de boetebevoegdheid van de AP bij management het nodige bewustzijn gecreëerd.

53. Respondenten kregen slechts toegang tot de gehele enquête voor zover ze werkzaam zijn (of na 1 september 2013 werkzaam waren) binnen de Rijksoverheid. Werknemers van de Rijksoverheid die geen ervaring hadden met het Toetsmodel PIA Rijksdienst kregen een verkorte versie van de enquête aangeboden met uitsluitend de vragen die niet specifiek over het Toetsmodel gingen.
54. Vraag 17 uit de enquête.
55. Vraag 18 uit de enquête.
56. Alle respondenten hebben de mogelijkheid gekregen om hun antwoorden nader toe te lichten.
57. Vraag 15 uit de enquête.
58. Vraag 16 uit de enquête.
59. Vraag 20 van de enquête.
60. Vraag 21 van de enquête.
61. Vraag 22 van de enquête.
62. Vraag 23 van de enquête.
63. Vraag 14 van de enquête.
65. Informatiebeveiligingsrisico's.
66. Vraag 19 van de enquête.
67. Vraag 24 van de enquête.
68. Vraag 25 van de enquête.

2 Format Enquêtevragenlijst Evaluatie Toetsmodel PIA Rijksdienst

Format Enquêtevragenlijst
Evaluatieonderzoek Toetsmodel PIA Rijksdienst

08. 04. 2016

Vragenlijst Evaluatieonderzoek Toetsmodel PIA Rijksdienst

Hartelijk dank voor uw medewerking aan het evaluatieonderzoek naar het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst. Privacy Management Partners voert dit onderzoek uit in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
Onderstaande vragen gaan zowel over uw ervaringen met het Toetsmodel als over mogelijke verbeteringen ervan. Met de term “Toetsmodel” bedoelen we hieronder uitsluitend de huidige versie, terwijl de term “PIA-instrument” meer in het algemeen verwijst naar zowel het huidige Toetsmodel als eventuele verbeterde versie of alternatieven.
Uw ervaringen binnen de overheid, specifiek met het Toetsmodel of met PIA’s in het algemeen, zijn voor ons van grote waarde. De resultaten van dit onderzoek zullen anoniem worden verwerkt. Desondanks bestaat een klein maar reëel risico op indirecte herleidbaarheid. Indien u op de hoogte wilt blijven van de uitkomst van dit onderzoek, kunt u bij de laatste vraag uw e-mail achterlaten. Dit zal het enige direct herleidbare persoonsgegeven zijn dat wij dan ook voor slechts zojuist omschreven doel gebruiken. Het invullen van deze vragenlijst neemt ongeveer 15 minuten in beslag.

Alvast bedankt voor uw deelname!

Introductievraag: Bent u werkzaam (of sinds 1 september 2013 werkzaam geweest) binnen de Rijksoverheid?

◯ Nee (dan sturen we u nu graag door).

◯ Ja, namelijk bij (onderdeel van de Rijksoverheid waarbij u werkzaam bent (geweest)):

Introductievraag: In welke rol heeft u vooral te maken gehad met het Toetsmodel PIA Rijksdienst (of een ander instrument voor een PIA)?

Vraag instructies: Onder ‘opdrachtgever’ verstaan we degene die formeel of feitelijk opdracht geeft tot het uitvoeren van een PIA; onder ‘uitvoerder’ verstaan we degene die het uitvoeren van een PIA organiseert of coördineert, dan wel zelf de PIA-vragen beantwoordt. Onder ‘toezichthouder’ verstaan we iemand die vanuit een staf- of toezichtsrol belang heeft bij de resultaten van een PIA, zoals een FG (functionaris gegevensbescherming) of CIO. ‘Anders, namelijk’ is van toepassing als u bijvoorbeeld externe adviseur bent, of nooit betrokken bent geweest bij een PIA.

☐ Opdrachtgever

☐ Uitvoerder

☐ Toezichthouder

☐ Anders (en/of toelichting), namelijk:

Ervaring met PIA’s: Bij hoeveel PIA’s bent u – in één of meer van de genoemde rollen – betrokken geweest?

◯ Geen

- ◯ 1 of 2
- ◯ 3 tot 5
- ◯ Meer dan 5

Ervaring met het Toetsmodel: Bent u betrokken geweest bij PIA's die werden uitgevoerd aan de hand van het Toetsmodel PIA Rijksdienst?

- ◯ Ja.
- ◯ Nee. Vragen 1 tot en met 13 gaan over het Toetsmodel PIA Rijksdienst en PIA's die zijn uitgevoerd aan de hand van het Toetsmodel. Indien u geen gebruik heeft gemaakt van het Toetsmodel voor het uitvoeren van een PIA sturen we u door naar vraag 14.

Vraag 1. Stelling: de vragen van het Toetsmodel zijn op de praktijk toegesneden.

Vraag instructies: In de vragen 1 tot en met 13 ziet u stellingen waarbij u aan mag geven in welke mate u het eens bent met de stelling. Stellingen 1 tot en met 6 hebben betrekking op het Toetsmodel PIA Rijksdienst. De overige stellingen hebben betrekking op het PIA-proces in het algemeen. U kunt kiezen uit de volgende antwoordmogelijkheden: 1: volledig mee oneens, 2: mee oneens, 3: enigszins mee oneens, 4: enigszins mee eens, 5: mee eens, 6: volledig mee eens en 7: weet ik niet/niet van toepassing/anders, namelijk…

- ☐ 1: Volledig mee oneens
- ☐ 2: Mee oneens
- ☐ 3: Enigszins mee oneens
- ☐ 4: Enigszins mee eens
- ☐ 5: Mee eens
- ☐ 6: Volledig mee eens
- ☐ Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 2. Stelling: de vragen van het Toetsmodel zijn begrijpelijk.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- ☐ 1: Volledig mee oneens
- ☐ 2: Mee oneens
- ☐ 3: Enigszins mee oneens
- ☐ 4: Enigszins mee eens
- ☐ 5: Mee eens
- ☐ 6: Volledig mee eens
- ☐ Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 3. Stelling: de vragenlijst van het Toetsmodel is volledig.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 4. Stelling: het Toetsmodel is een goed instrument om privacyrisico's in kaart te brengen.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 5. Stelling: het Toetsmodel is prettig om mee te werken.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 6. Stelling: De light versies zijn een zinvolle uitbreiding van het Toetsmodel.

Vraag instructies: In het Toetsmodel zijn drie 'light versies' opgenomen, in de zin dat drie soorten situaties beschreven worden waarin slechts een deel van de vragen beantwoord hoeven te worden. [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens

- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 7. Stelling: PIA's worden soms niet uitgevoerd omdat degene die ervoor verantwoordelijk is niet weet dat een PIA verplicht is.

Vraag instructies: Stellingen 7 tot en met 9 hebben betrekking op het proces van het uitvoeren van een PIA op basis van het Toetsmodel. [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 8. Stelling: de rolverdeling tussen de bij de PIA betrokken personen is helder.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 9. Stelling: het PIA-proces loopt in de praktijk goed.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens

- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 10. Stelling: de uitvoering van een PIA heeft geholpen bij het zicht krijgen op privacyrisico's.

Vraag instructies: Stellingen 10 tot en met 13 hebben betrekking op het effect van het uitvoeren van een PIA op basis van het Toetsmodel. [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 11. Stelling: de uitvoering van een PIA had een corrigerende/richtinggevende functie.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 12. Stelling: de uitvoering van een PIA heeft geleid tot een meer zorgvuldige omgang met persoonsgegevens.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- [ ] 1: Volledig mee oneens
- [ ] 2: Mee oneens
- [ ] 3: Enigszins mee oneens
- [ ] 4: Enigszins mee eens
- [ ] 5: Mee eens
- [ ] 6: Volledig mee eens
- [ ] Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 13. de uitvoering van een PIA heeft bijgedragen aan het vergroten van het draagvlak voor het project.

Vraag instructies: [Geef aan in welke mate u het eens bent met de stelling]

- ☐ 1: Volledig mee oneens
- ☐ 2: Mee oneens
- ☐ 3: Enigszins mee oneens
- ☐ 4: Enigszins mee eens
- ☐ 5: Mee eens
- ☐ 6: Volledig mee eens
- ☐ Weet ik niet/niet van toepassing/anders (en/of toelichting), namelijk

Vraag 14. Geef aan in welke mate de genoemde aspecten aanwezig waren bij de verslaglegging over de uitkomsten van PIA's uitgevoerd op basis van het Toetsmodel.

Vraag instructies: Mocht u een eigen toelichting willen toevoegen, kunt u dit bij de laatste (open) vraag invullen.

	Niet	Beperkt	Ruimschoots	Volledig	Weet ik niet/N.v.t.
Een beschrijving van systemen en processen	◯	◯	◯	◯	◯
Een beschrijving van persoonsgegevens	◯	◯	◯	◯	◯
Een juridische analyse	◯	◯	◯	◯	◯
Een overzicht van de privacyrisico's	◯	◯	◯	◯	◯
Een overzicht van de informatiebeveiligingsrisico's	◯	◯	◯	◯	◯
Aanbevelingen ter voorkoming/het mitigeren van privacyrisico's	◯	◯	◯	◯	◯
Aanbevelingen ter voorkoming/het mitigeren van informatiebeveiligingsrisico's	◯	◯	◯	◯	◯

Vraag 15. De beste vorm voor een PIA-instrument vind ik:

- ☐ Eén integraal instrument, zoals dat nu het geval is.
- ☐ Twee gescheiden instrumenten, één gericht op beleid en wetgeving, en één gericht op processen en systemen waarbij persoonsgegevens wordt verwerkt.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 16. De beste vorm voor een PIA-instrument vind ik:

Vraag instructies: In zijn huidige vorm bestaat het Toetsmodel uit een vaste lijst vragen. Een alternatief is om de alleen de voorwaarden te specificeren waaraan een PIA moet voldoen.

- ☐ Een vaste lijst van vragen die moeten worden beantwoord, waarmee uniformiteit tussen de PIA's wordt bewerkstelligd (met het risico dat sommige vragen irrelevant zijn voor mijn casus).
- ☐ Een beschrijving van de randvoorwaarden waaraan een goede PIA moet voldoen en op basis waarvan ik mijn eigen concrete PIA kan vormgeven.
- ☐ De twee mogelijkheden hierboven allebei als optie bieden.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 17. De beste manier om het PIA-proces in goede banen te leiden vind ik:

Vraag instructies: In zijn huidige vorm kent het Toetsmodel een toelichting die beschrijft hoe een PIA op basis van het Toetsmodel moet worden uitgevoerd. Een alternatief is om de vragen zo vorm te geven dat zij de uitvoerder van de PIA min of meer automatisch door het proces leiden. Een andere optie is het open laten van de PIA-methodiek.

- ☐ Een losse toelichting bij het PIA-instrument die het PIA-proces beschrijft.
- ☐ Een vragenlijst die de uitvoerder min of meer automatisch door het PIA-proces leidt.
- ☐ Elke instantie mag haar eigen PIA-methodiek ontwikkelen.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 18. Heeft u behoefte aan duidelijke criteria wanneer u een PIA moet doen?

Vraag instructies: Via deze vraag willen we erachter komen aan welke hulpmiddelen ter uitvoering van de PIA u behoefte heeft. Denk bij een pre-scan aan een aantal vragen die u helpen te beoordelen of een PIA daadwerkelijk uitgevoerd moet worden. Mogelijk heeft u aan een handleiding voldoende of is er geen behoefte aan een hulpmiddel aangezien het voor u duidelijk is wanneer u een PIA moet uitvoeren.

- ☐ Ja, in de vorm van een pre-scan.
- ☐ Ja, in de vorm van een handleiding.
- ☐ Nee, dat is duidelijk genoeg.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 19. Voor wie moeten de definitieve resultaten van een uitgevoerde PIA volgens u beschikbaar zijn?

Vraag instructies: Middels deze vraag willen we nagaan aan welke partijen de uitkomsten van een PIA beschikbaar zouden moeten worden gesteld. Het gaat hier specifiek om het eindproduct van een uitgevoerde PIA, niet om tussentijdse concepten, memo's, verslagen enz.

- ☐ Voor iedereen (openbaar).
- ☐ Voor het (project)team, het MT, de politieke leiding en andere betrokken departementen c.q. Rijksdiensten.
- ☐ Voor (project)team, het MT en de politieke leiding.
- ☐ Voor (project)team en het MT.

- ☐ Alleen voor het (project)team.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 20. De komende Europese privacyverordening vereist dat, waar passend, de personen van wie persoonsgegevens worden verwerkt (of organisaties die hen vertegenwoordigen) worden geconsulteerd bij de uitvoering van de PIA. Bij vertegenwoordigende organisaties kunt u denken aan bijvoorbeeld de vakbonden of organisaties die zich inzetten voor mensenrechten. In hoeverre denkt u aan deze verplichting te kunnen voldoen?

- ☐ Ik zou niet weten welke (organisaties van) betrokkenen ik kan consulteren.
- ☐ Ik weet welke (organisaties van) betrokkenen ik kan consulteren, en kan dat organiseren.
- ☐ Ik vind consultatie niet wenselijk.
- ☐ Ik weet het niet.
- ☐ Anders, (en/of toelichting) namelijk:

Vraag 21. Als ik een workshop zou organiseren voor de uitvoering van een PIA voor beleid of wetgeving, dan zou ik in ieder geval de volgende personen erbij willen betrekken (Let op: Deze vraag richt zich alleen op PIA's voor beleid of wetgeving):

Vraag instructies: Deze en de volgende vraag gaan over het houden van een workshop als onderdeel van een PIA. Met een workshop bedoelen wij: een bijeenkomst waarin deelnemers die vanuit verschillende invalshoeken inzichten kunnen bijdragen gezamenlijk tot antwoorden op de PIA-vragen proberen te komen. [Meerdere antwoorden mogelijk]

- ☐ Een Wbp-coördinator/privacy-expert
- ☐ Een (wetgevings)jurist
- ☐ Betrokken beleidsmedewerkers
- ☐ Betrokken (project)medewerkers
- ☐ Betrokken ketenpartner(s)
- ☐ De FG
- ☐ De CIO/iemand van het CIO-office
- ☐ Een procesbegeleider
- ☐ Niet van toepassing: het houden van workshops lijkt mij geen effectieve aanpak voor de uitvoering van een PIA
- ☐ Ik weet het niet
- ☐ Anders, namelijk (of toelichting)

Vraag 22. Als ik een workshop zou organiseren voor de uitvoering van een PIA voor een proces of systeem, dan zou ik in ieder geval de volgende personen

erbij willen betrekken: (Let op: Deze vraag richt zich alleen op PIA's voor voor processen of systemen):

Vraag instructies: Deze vraag gaat net als de vorige over het houden van een workshop als onderdeel van een PIA. [Meerdere antwoorden mogelijk]

- ☐ Een Wbp-coördinator/privacy-expert
- ☐ Een jurist
- ☐ Een informatiebeveiligingsexpert
- ☐ Vertegenwoordiger van de gebruiker(s) van het systeem
- ☐ Betrokken beleidsmedewerkers
- ☐ Betrokken (project)medewerkers
- ☐ Betrokken ketenpartner(s)
- ☐ Eventuele bewerker(s)
- ☐ De FG
- ☐ De CIO/iemand van het CIO-office
- ☐ Een procesbegeleider
- ☐ Niet van toepassing: het houden van workshops lijkt mij geen effectieve aanpak voor de uitvoering van een PIA
- ☐ Ik weet het niet
- ☐ Anders, namelijk (of toelichting)

Vraag 23. U mag 10 punten verdelen over de genoemde opties voor het verbeteren van de manier waarop er binnen de Rijksoverheid wordt omgegaan met de privacyrisico's van nieuw beleid of wetgeving, of nieuwe systemen of processen. Hoe meer punten, hoe meer waarde u eraan hecht dat de betreffende optie gerealiseerd wordt.

Vraag instructies: Mocht u een eigen toelichting willen toevoegen, kunt u dit bij de laatste (open) vraag invullen.

Toewijzen: 10 Punten

Beschikbaar stellen van een interactief digitaal PIA-instrument.	
Aanbieden van PIA-trainingen.	
Aanbieden van benchmarks voor de kwaliteit van PIA's.	
Aanbieden van een helpdesk voor vragen en begeleiding.	
Aanbieden van een pool van PIA-experts die kunnen worden ingeschakeld bij de uitvoering.	
Extra antwoord	
Anders.	

Vraag 24. In welke mate brengt de toepassing van het Toetsmodel de onderstaande effecten teweeg? Gelieve de effecten hoger te plaatsen naarmate zij in uw ervaring vaker optreden.

Groter privacybewustzijn in de organisatie.	
Meer inzicht in de details van de verwerkingen van persoonsgegevens.	
Meer inzicht in de privacyrisico's van het beleid en/of de verwerking.	
Meer inzicht in de informatiebeveiligingsrisico's.	
Overeenstemming over de benodigde waarborgen.	
Tijdige bijsturing of stopzetten van het project.	
Anders, (en/of toelichting) namelijk:	

Vraag 25. Welke van de onderstaande effecten zou een PIA-instrument vooral moeten hebben? Gelieve de effecten hoger te plaatsen naarmate het volgens u belangrijker is dat zij optreden.

Groter privacybewustzijn in de organisatie.	
Inzicht in de details van de verwerkingen van persoonsgegevens.	
Meer inzicht in de privacyrisico's van het beleid en/of de verwerking.	
Meer inzicht in de informatiebeveiligingsrisico's.	
Overeenstemming over de benodigde waarborgen.	
Tijdige bijsturing of stopzetten van het project.	
Anders, (en/of toelichting) namelijk:	

Wat wilt u verder nog kwijt over PIA's bij de Rijksoverheid en/of het Toetsmodel PIA Rijksdienst?

Indien u op de hoogte wilt blijven van de uitkomst van dit onderzoek, kunt u (alleen voor dit doel) uw e-mail achterlaten in onderstaand antwoordveld.

Bijlage IV – Toetsmodel

Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst

A. Ten geleide

1. *Wat is een PIA?*

1. Een Privacy Impact Assessment (PIA) is een hulpmiddel om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen. Het PIA-toetsmodel is specifiek gericht op de Rijksdienst en bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen.
2. De PIA heeft de vorm van een toetsmodel/vragenlijst. Op die lijst staan zowel feitelijke en technische vragen als vragen die zijn gebaseerd op nationale en Europese juridische vereisten. Het richt zo in een vroegtijdig stadium en op hoofdlijnen de aandacht op alle onderdelen van de beoogde verwerking van persoonsgegevens die aandacht en uitwerking behoeven.
3. Een PIA is geen vrijblijvende enquête. In het bijzonder is de vragenlijst inhoudelijk gezien zowel richtinggevend als corrigerend bedoeld. Daarnaast moet het beantwoordingsproces als zodanig ook bewustwording stimuleren van de uiteenlopende privacy-aspecten waarmee rekening moet worden gehouden bij ontwikkeling van een wetgeving en beleid en in dat kader te ontwikkelen ICT-systemen en databestanden.
4. Een PIA is richtinggevend in de zin dat de (uitputtende) vragenreeks kan wijzen op relevante privacy-risico's die in de vroege fase van beleids- of systeemontwikkeling (wellicht nog) niet zijn onderkend. Als dat het geval is, moet de betreffende vraag zo worden opgevat dat het noodzakelijk is om deze aspecten alsnog in de uitwerking mee te nemen.
5. Een PIA is ook corrigerend. Door de vragenvolgorde zal het vaak nodig zijn voorlopige antwoorden op eerdere vragen te heroverwegen, en vervolgens voor een andere (minder privacy-inperkende) oplossing te kiezen. Het zal dan ook geregeld voorkomen dat in een eerder stadium van beleids- of systeemontwikkeling overwogen opties en oplossingen bij nadere beschouwing niet goed genoeg kunnen worden onderbouwd vanwege de hiermee gepaard gaande privacy-risico's.
6. Vanwege het richtinggevende en corrigerende karakter van een PIA zal het invullen van de vragenlijst vaak een dynamisch proces zijn, waarbij concept-(beleids)oplossingen of het concept-functionele systeemontwerp geleidelijk worden aangescherpt.
7. Een PIA moet worden gehanteerd naast, en in afstemming met andere hulpmiddelen voor ontwikkeling van wetgeving en beleid, en daarmee gepaard gaande bouw van ICT-systemen en aanleg van databestanden. Een PIA komt dus niet in de plaats van deze bestaande instrumenten, en is niet bedoeld daarmee te overlappen.
8. Indien de PIA wordt uitgevoerd in het kader van ontwikkeling van beleid dat moet resulteren in wetgeving, moet in de fase van juridische verfijning van het wetsvoorstel de in het IAK opgenomen Leidraad afstemming op de Wbp worden gebruikt.
9. Indien de PIA wordt uitgevoerd in het kader van ontwikkeling van beleid waarmee (ook) de aanleg van databestanden of de bouw van ICT-systemen wordt voorzien, moet ook rekening worden gehouden met de beheersmaatregelen zoals beschreven in het handboek portfoliomanagement Rijk voor projecten met een grote ICT-component.
10. Beantwoording van de PIA-vragenlijst resulteert in een geschreven document.

2. *Wanneer is verwerking van persoonsgegevens door de Rijksdienst, inclusief ZBO noodzakelijk (en komt een PIA aan de orde)*?

1. Gebruik van persoonsgegevens, waaronder door de overheid, vormt in veel gevallen een inperking van het grondrecht van bescherming van de persoonlijke levenssfeer (artikel 10, leden 2 en 3 Grondwet, artikel 8 EVRM, artikel 8 EU-Grondrechtenhandvest).
2. Zodra hieraan wordt gedacht in het kader van ontwikkeling van beleid en wetgeving, en de daarmee gepaard gaande bouw van ICT-systemen en aanleg van databestanden, moet eerst worden vastgesteld of verwerking van persoonsgegevens noodzakelijk is voor het te bereiken doel. Hierbij speelt zowel de vraag naar subsidiariteit als proportionaliteit.
3. Voor wat betreft subsidiariteit is de (voor)vraag: is het alleen door middel van verwerking van persoonsgegevens mogelijk het gewenste beleidsmatige resultaat te bereiken? Zijn er ook effectieve praktische of technische alternatieven die helemaal niet ingrijpen op de privacy? (Hierbij kan bijvoorbeeld worden gedacht aan het niet verwerken van op de persoon herleidbare gegevens voor aspecten van het voorstel die enkel trends of algemene patronen willen vastleggen). Indien alternatieven voor verwerking van persoonsgegevens met hetzelfde beleidsmatige resultaat voorhanden zijn, moet daarvoor worden gekozen.
4. Voor ontwikkeling van beleid en wetgeving kan voor het beantwoorden van deze vragen naar de subsidiariteit van de verwerking van persoonsgegevens ook gebruik worden gemaakt van de in het IAK opgenomen checklist afstemming op (internationale) (klassieke) grondrechten.
5. Indien de (voorlopige) bevinding is dat alternatieven voor verwerking van persoonsgegevens niet bestaan, is het zaak het PIA-toetsmodel ter hand te nemen. Zo kunnen alle aan proportionaliteit gelieerde vragen van de voorziene verwerking van persoonsgegevens helder in beeld worden gebracht en kunnen oplossingen worden geformuleerd die niet verder gaan dan nodig om het gewenste resultaat te bereiken (Hierbij kan bijvoorbeeld worden gedacht aan het differentiëren van maatregelen (is verwerking van dezelfde persoonsgegevens nodig voor alle aspecten van het beleidsvoorstel?), of het toestaan van de mogelijkheid van een “opt-out” aan betrokkenen in bepaalde specifieke omstandigheden).
6. Een PIA moet dus zo vroeg mogelijk in het proces van de vorming van beleid dat verwerking van persoonsgegevens voorziet, al dan niet gepaard gaande met wetgeving of bouw van ICT-systemen, worden gebruikt.

3. *Hoe moet een PIA worden gehanteerd?*

1. Beleids- en wetgevingsinitiatieven binnen de Rijksdienst om persoonsgegevens te verwerken kennen vele gedaanten. Aan de ene kant kan het gaan om een geheel nieuw databestand of systeem waarin een nieuwe verzameling persoonsgegevens voor een nieuw doel zal worden verwerkt. Aan de andere kant kan het gaan om het toevoegen van een nieuw type persoonsgegevens aan de verwerking in een al bestaand ICT-systeem, of het koppelen van verschillende al bestaande databestanden of systemen om een nieuw doel te bereiken. Ook kan het gaan om nieuwe vormen van verstrekking, uitwisseling, openbaarmaking en (meervoudig) gebruik van gegevens.
2. De PIA-vragenlijst is opgesteld voor het gehele spectrum van nieuwe vormen van gegevensverwerking. Het met het aflopen van de vragen te ondervangen privacy-risico zal echter sterk afhangen van de aard van het beleids- of wetsvoorstel of het voorgenomen ICT-systeem of databestand. Het zal dus per geval verschillen welke van de PIA-vragen moeten worden beantwoord.

3. Het is niet nodig om de gehele vragenlijst af te werken als het gaat om:
   - uitbreiding van het databestand binnen een bestaand ICT-systeem (volstaan kan worden met beantwoording van de vragen in secties I en IV)
   - gebruik van een bestaand databestand of ICT-systeem voor aanvullende of nieuwe doelen (volstaan kan worden met beantwoording van de vragen in sectie II en IV)
   - koppeling van verschillende al bestaande databestanden of ICT-systemen voor bestaande of aanvullende of nieuwe doelen (volstaan kan worden met beantwoording van de vragen in secties II-V)

   Vanzelfsprekend is het bij het uitvoeren van een dergelijke "PIA-light" verstandig terug te grijpen op eventuele eerdere stukken (uitgevoerde PIAs, andere impact assessments, toelichtingen).
4. In alle andere gevallen moet, mede gezien de eerder genoemde samenhang tussen de vragen, en het richtinggevende en corrigerende karakter van de PIA, wel de gehele vragenlijst worden afgelopen.
5. De uiteindelijke beantwoording van de PIA-vragen zal als basis en bron moeten dienen voor technische, beleidsmatige en juridische verantwoording van keuzen (zie daarover nader onder 5).

4. *Wie? Uitvoering en afstemming*

1. De PIA-vragenlijst moet worden ingevuld door de beleidsmedewerker of wetgevingsjurist van de Minister die, of het ZBO dat "verantwoordelijke" is of zal zijn voor een verwerking van persoonsgegevens in de zin van de Wet bescherming persoonsgegevens.
2. Van "verantwoordelijkheid" is sprake, in de bewoordingen van de Wbp, als dit onderdeel van de Rijksdienst de entiteit is die het doel van en de middelen voor de verwerking van persoonsgegevens vastlegt.
3. Een PIA hoeft niet te worden ondernomen door beleidsmakers of wetgevingsjuristen van het ministerie of het onderdeel van de Rijksdienst dat slechts als "bewerker" optreedt in de zin van de Wbp, d.w.z. als slechts in opdracht van een verantwoordelijke wordt gehandeld. Neem contact op met de juridische afdeling van uw Ministerie als hierover onduidelijkheid bestaat.
4. De Functionaris Gegevensbescherming (FG) is binnen uw departement verantwoordelijk voor het onafhankelijk toezicht op toepassing en naleving van de Wet bescherming persoonsgegevens. U kunt met de FG contact opnemen voor advies tijdens de beantwoording van de vragenlijst of over de resultaten van de beantwoording. De FG kan aandachtspunten signaleren en risico's helpen duiden.
5. Als uw beleids- of wetgevingsvoorstel betrekking heeft op de bouw van een ICT-systeem of het aanleggen van een databestand, neem dan ook tijdig contact op met uw departementale Chief Information Officer (CIO). Deze geeft een oordeel bij de start of tussentijdse wijziging van een project, zoals opgenomen in de I-strategie. Onderdeel hierin is de beoordeling of in het projectplan is opgenomen of er binnen het project sprake is van het opnemen van privacygevoelige gegevens of van het koppelen of verrijken van data, en of daarbij beargumenteerd is of een PIA gewenst is.

5. Gebruik en verantwoording PIA-resultaten

1. Een serieus uitgevoerde PIA zal richtinggevend en corrigerend hebben gewerkt. Plannen zijn toegespitst en uitgewerkt. Dit heeft tot gevolg dat bij voorbereiding van wetgeving, beleid en overheidsICT-systemen privacy-aspecten als zodanig onderdeel zijn geworden van het afwegingsproces. Omdat hierop gebaseerde aanpassingen hiermee al zullen zijn meegenomen in de uiteindelijke beantwoording van de PIA-vragen moeten alleen de definitieve antwoorden worden gebruikt bij de verdere ontwikkeling van beleid en systemen.
2. De afwegingen en keuzes die uit de uiteindelijke antwoorden blijken zullen per wets- of beleidsvoorstel danwel ICT-systeem verschillen. Voor de verantwoording van het uiteindelijke gebruik van persoonsgegevens zal tevens moeten worden verwezen naar eerdere beleidskeuzes en oplossingen in andere contexten. Ook nieuwe aspecten, of elementen die afwijken van eerder gemaakte keuzes (bv. meer gegevens dan voorheen, een ander systeem dan voorheen, etc.), zullen nadere toelichting verdienen.
3. Resultaten van een PIA moeten worden gezonden aan de betrokken FG en de CIO. Afhankelijk van de context waarin de PIA wordt uitgevoerd, worden de resultaten echter op verschillende manieren verwerkt.
4. Waar het gaat over beleid dat de bouw van ICT-systemen of de aanleg van databestanden voorziet, zal de FG op basis hiervan advies kunnen geven bij het bepalen van de nodige maatregelen en waarborgen die moeten worden neergelegd in beleidsregels, aanwijzingen, gebruikshandleidingen en procedures. Daarnaast zullen CIOs de resultaten kunnen gebruiken voor advisering over informatiebeveiliging en systeemontwerp. Ook kunnen de PIA resultaten input vormen voor een eventuele melding van de voorgenomen verwerking aan het CBP of de FG, die volgens de daarvoor geldende regels openbaar gemaakt wordt.
5. Bij wetgeving wordt over PIA-resultaten een passage opgenomen in de toelichting. Daarin kan dan een samenvatting worden gegeven van de belangrijkste afwegingen en keuzes. Het ligt voor de hand deze passage toe te voegen aan de al standaard op te nemen beschouwing over het grondrechtelijke kader en de toetsing aan de Wet bescherming persoonsgegevens (zie ook hierboven, onder A). Hoewel een volledig gestandaardiseerde verantwoordingsparagraaf dus niet kan worden gegeven, zou een model-element van deze MvT-paragraaf kunnen zijn:
   “Gezien de aard van dit voorstel is in de fase van beleidsontwikkeling een Privacy Impact Assessment uitgevoerd (zie ook Kamerstukken I 2010/11, 31051, nr. D; motie-Franken). Met behulp hiervan is de noodzaak van gegevensverwerking bekeken, en 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 de betrokkenen. [Beschrijving specifieke aspecten en de in dit geval gemaakte belangenafweging]”

B. Vragenlijst

Vooraf : *Gegevensverwerking is sterk juridisch ingekaderd. Anderzijds wordt de tekst van de Wet bescherming persoonsgegevens (Wbp) vaak juist als abstract en ondoorgrondelijk ervaren. In dit licht bevat de onderstaande vragenlijst zowel praktische als meer juridisch getinte vragen. De praktische vragen zijn ervoor bedoeld om het hele traject van gegevensverwerking, en daarbij betrokken instanties, goed in kaart te brengen. Waar het gaat om juridisch getinte vragen luistert de formulering van de vragen nauw. In dat geval is zoveel mogelijk geprobeerd deze toe te lichten en voorbeelden toe te voegen. Indien er onduidelijkheid bestaat over de inhoud van de vraag, is het raadzaam daarover contact op te nemen met de Functionaris Gegevensbescherming van uw ministerie of de juridische afdeling.*

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

> *Toelichting: Definitie persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon (art. 1 Wbp).*
> *Definitie bijzondere (gevoelige) persoonsgegevens: gegevens over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksueel leven, lidmaatschap van een vakvereniging, strafrechtelijk verleden; Cf. art. 16 Wbp*
> *Definitie: Een verantwoordelijke is een natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vastlegt.*
> *N.B. Als uw organisatie slechts als bewerker (degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen) optreedt, moet deze vragenlijst door de verantwoordelijke en niet door u worden ingevuld.*
> *Definitie verwerking: 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, uitwisselen of vernietigen van persoonsgegevens.*

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

> *Toelichting:Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, gokverslaving, prestaties op school of werk of relatieproblemen.*

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

> *Toelichting: hieronder vallen bijvoorbeeld minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking, klokkenluiders of informanten voor politie of het OM.*

2c.Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

> *Toelichting:De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Hierbij moet er rekening mee worden gehouden dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.*

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Toelichting: Dit type gegevens is weliswaar niet formeel aangemerkt als bijzonder persoonsgegeven in de dataprotectierichtlijn 95/46 en op basis daarvan in de Wbp, maar wordt in de nationale en Europese rechts- en toepassingspraktijk inmiddels wel als zodanig behandeld. Aanhangige Europese voorstellen voor aanpassing van dataprotectieregelgeving continueren deze trend door verwerking van biometrische gegevens als specifiek risico aan te merken.

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Toelichting: De Wbp (art 24) bepaalt dat een bij de wet voorgeschreven nummer ter identificatie van een persoon bij verwerking van persoonsgegevens slechts verwerkt wordt ter uitvoering van de desbetreffende wet of doeleinden bij de wet bepaald. Raadpleeg zonodig het Besluit gebruik sofi-nummer Wbp van 15 augustus 2001.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

Toelichting: De Wbp legt het zogenaamde principe van dataminimalisatie neer. Persoonsgegevens mogen slechts worden verwerkt als daarvoor een noodzaak bestaat (art 8). Art. 11, lid 1 bepaalt daarnaast dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (relevantie-eis). Verder is van belang dat verwerking van gevoelige persoonsgegevens in principe verboden is (art. 16-23 Wbp), en slechts onder strikte(re) voorwaarden is toegestaan.

4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Toelichting: Anonimisering betekent verwijdering van alle direct en uniek identificerende gegevens.

Pseudonimisering betekent systematische vervanging van direct identificerende gegevens van personen door bv. een code waardoor in de toekomst bepaalde geautoriseerde partijen nog steeds gegevens kunnen toevoegen, maar terugleiding tot de specifieke persoon niet meer mogelijk is. Dit kan bv. door persoonsgegevens direct na verzameling in een bepaald algoritme om te zetten, waardoor analyse en vergelijking mogelijk blijft maar de bron van de gegevens als zodanig in principe niet meer is op te roepen.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Toelichting:Inventariseer alle verwerking van persoonsgegevens en verantwoordelijkheden en geef het geheel bijvoorbeeld door middel van een grafische weergave overzichtelijk weer zodat het hele traject van gegevensverwerking inzichtelijk wordt.

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Toelichting: De Wbp (art. 7) bepaalt dat persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen mogen worden verzameld. Zo kan bijvoorbeeld worden aangegeven in wetgeving dat persoonsgegevens worden verwerkt voor het vastomlijnde doel van tegengaan van illegale immigratie. De verwerking dient gerechtvaardigd te zijn door één van de gronden van artikel 8 Wbp. Indien meerdere doelen worden nagestreefd met het verzamelen van de persoonsgegevens moeten die allemaal worden genoemd, en moet voor elk van die doelen worden gerechtvaardigd waarom de (hele) voorziene set van persoonsgegevens hiervoor noodzakelijk is.

2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

Toelichting: De Wbp legt het zogenaamde principe van dataminimalisatie neer. In art. 11, lid 1 bepaalt het dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn. Dit betekent dat als de gegevens die wordt verwerkt in een bestaand systeem wordt uitgebreid, voor elk van de nieuw te verwerken persoonsgegevens een rechtvaardiging moet bestaan. Zie voor een beoordeling van de toe te voegen gegevens ook vragen I.1-4 hierboven.

3. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Toelichting: De Wbp (art. 9, lid 1) bepaalt dat persoonsgegevens niet verder mogen worden verwerkt (bv. in de vorm van koppeling of vergelijking met andere persoonsgegevens, of toevoeging van andere persoonsgegevens voor het bereiken van een nader doel) op een wijze die onverenigbaar is met het/de doel(en) waarvoor ze in eerste instantie zijn verkregen. Loop het hele voorziene traject van de persoonsgegevens na en geef bij elk onderdeel aan of er sprake is van een ander doel dan waarvoor de gegevens zijn verzameld.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

Toelichting: De Wbp (art. 62) maakt het mogelijk om een functionaris voor de gegevensbescherming (FG) te benoemen. Deze functionaris ziet toe op de verwerking van persoonsgegevens. Het toezicht door deze functionaris strekt zich uit tot de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd. De functionaris kan aanbevelingen doen aan de verantwoordelijke die strekken tot een betere bescherming van de gegevens die worden verwerkt. Volgens art. 27, lid 3 moeten voorgenomen verwerkingen aan de FG worden gemeld. Als er geen FG is, moet dit gebeuren aan het Cbp.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Toelichting: zie toelichting bij vragen II.2 en II.3. Het kan bijvoorbeeld gaan om het plannen van een intern evaluatie-moment, of een externe evaluatie.

Kwaliteit

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Toelichting: De Wbp (art. 11, lid 2) bepaalt dat maatregelen moeten worden genomen om er voor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zijn worden verzameld of verder verwerkt, juist en nauwkeurig zijn.

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Toelichting: De Wbp (art. 42, lid 1) stelt dat niemand aan een besluit kan worden onderworpen waaraan rechtsgevolgen zitten voor hem indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid.

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Toelichting: De Wbp (art. 1, d) merkt als verantwoordelijke aan de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Toelichting: De Wbp (art. 9, lid 4) bepaalt dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat. Van een dergelijke geheimhoudingsplicht is bijvoorbeeld soms sprake voor medici en (jeugd)hulpverleners.

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Toelichting: De kenmerken van de verwerking moeten altijd beschikbaar zijn als voorwaarde om als verantwoordelijke "in control" te kunnen zijn, en in het bijzonder in verband met de meld- en inlichtingenplicht t.b.v. betrokkenen (artikel 27, eerste lid, Wbp, en artikel 30, lid 3, Wbp).

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Toelichting: De Wbp (art. 76) bepaalt dat persoonsgegevens slechts naar een land buiten de EU en EER mogen worden doorgegeven indien dat land een passend niveau van gegevensbescherming waarborgt.
Voor wat betreft de VS heeft de Europese Commissie bepaald dat organisaties die zich hebben verplicht tot naleving van de zogenaamde safe harbour principles ook geacht worden een passend beschermingsniveau te waarborgen. Een volledige lijst van Commissie-besluiten over de adequaatheid van het beschermingsniveau in overige derde landen (zoals bijvoorbeeld Israel, Argentinië en Australië) is te vinden op de volgende website: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

IV. Beveiliging en bewaring/vernietiging

Beveiliging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging ?

Toelichting: De Wbp (art. 13) vereist dat passende technische en organisatorische maatregelen worden genomen om persoonsgegevens te beveiligen tegen enige vorm van onrechtmatige verwerking.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

Toelichting: De Wbp (art. 14, lid 1) verplicht de verantwoordelijke ervoor zorg te dragen dat een bewerker, indien die (een deel van) de verwerking op zich neemt, voldoende technische en organisatorische beveiligingsmaatregelen neemt. Conform lid 2 moet hiervoor een bewerkersovereenkomst worden opgesteld. Er moet op basis van de Wbp toezicht plaatsvinden op de naleving van de maatregelen (artikel 14, lid 1, Wbp).

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

Toelichting: Voor het bepalen van het juiste risiconiveau kan worden gekeken naar CBP, "Richtsnoeren Beveiliging van Persoonsgegevens", 2013, op: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Bewaring/vernietiging

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Toelichting: De Wbp (art. 10, lid 1) geeft aan dat persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verder verwerkt.

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

V. Transparantie en rechten van betrokkenen

Transparantie

1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Toelichting: De hier bedoelde transparantieverplichting is te onderscheiden van (en komt bovenop) het wettelijke kenbaarheidsvereiste (verslaglegging van het doel van een gegevensverwerking in wetgeving zelf). Het doel van deze transparantieverplichting is betrokkenen te informeren over verwerking op een plaats/moment gelieerd aan de (voorgenomen) verwerking. Is er bijvoorbeeld op het formulier informatie opgenomen over de doeleinden van het verzamelen van de gegevens? Of is voorzien in borden langs de weg waarmee camera-controles worden aangekondigd?

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

Toelichting: De Wbp (art. 33) stelt specifieke regels over deze vorm van informatieverstrekking aan betrokkenen. De hier bedoelde transparantieverplichting is te onderscheiden van (en komt bovenop) het wettelijke kenbaarheidsvereiste (verslaglegging van het doel van een gegevensverwerking in wetgeving zelf). Het doel van deze transparantieverplichting is betrokkenen te informeren, al dan niet op diens verzoek, over verwerking op een plaats/moment gelieerd aan de (voorgenomen) verwerking.

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Toelichting: De Wbp (art. 34) stelt regels over informatieverstrekking aan betrokkenen. De hier bedoelde transparantieverplichting is te onderscheiden van (en komt bovenop) het wettelijk kenbaarheidsvereiste (verslaglegging van het doel van een gegevensverwerking in wetgeving zelf). Het doel van deze transparantieverplichting is betrokkenen te informeren over verwerking op een plaats/moment gelieerd aan de (voorgenomen) verwerking.

<u>Rechten van betrokkenen</u>

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Toelichting:Overeenkomstig artikel 8, lid 1 Wbp is ondubbelzinnige toestemming van betrokkene een van de mogelijke rechtvaardigingsgronden voor verwerking van persoonsgegevens. Dergelijke toestemming moet vrij, specifiek en geïnformeerd zijn gegeven.

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Toelichting: De Wbp (art. 35, leden 1 en 2) geeft de betrokkene het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt. Artikel 35, lid 3, stelt dat aan derden die mogelijk bedenkingen hebben tegen een dergelijke mededeling, vooraf in de gelegenheid moeten worden gesteld om hun zienswijze te geven behalve als dit een onevenredige inspanning zou vergen.

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Toelichting: De Wbp (art. 36) biedt een recht op correctie of afscherming, en ook een recht op verzet tegen verwerking in verband met bijzondere persoonlijke omstandigheden (art. 40).

Bijlage V – Geïnterviewden

- *Aafke Stuijt* (Ministerie van Financiën)
- *Alex Commandeur* (Autoriteit Persoonsgegevens)
- *Aramis Jean Piere* (Dienst Uitvoering Onderwijs)
- *Carine Zandee* (Ministerie van Financiën)
- *Diana van Driel* (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
- *Dirk Schravendeel* (PBLQ)
- *Erik van der Zeeuw* (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
- *Fieke van der Klugt* (voormalig Ministerie van Volksgezondheid, Welzijn en Sport, nu Ministerie van Sociale Zaken en Werkgelegenheid)
- *Hans Franken* (voormalig Eerste Kamerlid, indiener Motie Franken)
- *Hatice Dogan* (Sociale Verzekeringsbank)
- *Jan de Zeeuw* (Ministerie van Economische Zaken)
- *Jan Visscher* (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, geïnterviewd in hoedanigheid als lid van GroepsOndernemingsRaad BZK)
- *Jan-Peter Loof* (College voor de Rechten van de Mens)
- *Jessica Vuijk* (Ministerie van Infrastructuur en Milieu)
- *Kees Meesters* (Ministerie van Veiligheid en Justitie)
- *Lester von Meijenfeldt* (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
- *Maaike Vorselen* (Rijksoverheid, geïnterviewd in hoedanigheid als lid van GroepsOndernemingsRaad BZK)
- *Marcel Griffioen* (Ministerie van Onderwijs, Cultuur en Wetenschap)
- *Mariska Zwinkels* (Ministerie van Onderwijs, Cultuur en Wetenschap)
- *Marlies van Eck* (Belastingdienst)
- *Mathijs Raijmakers* (Raad van State)
- *Nathalie Falot* (Ministerie van Veiligheid en Justitie (gedetacheerd))
- *Peter Hustinx* (voormalig Europese toezichthouder voor gegevensbescherming)
- *Pieter de Groot* (Ministerie van Veiligheid en Justitie en Ministerie van BZK)
- *Reinier Ter Kuile* (voormalig Ministerie van Veiligheid en Justitie)
- *Renée van Schoonhoven* (Ministerie van Onderwijs, Cultuur en Wetenschap)
- *Rudolph Kroes* (voormalig Ministerie van Financiën/Belastingdienst)
- *Saskia Kroon* (Ministerie van Onderwijs, Cultuur en Wetenschap)
- *Vincent Böhre* (Stichting Privacy First)
- *Vincent Cozijn* (voormalig Ministerie van Defensie)

PRIVACY
MANAGEMENT
PARTNERS

bezoekadres
Vondellaan 106
3521 GH Utrecht

postadres
Postbus 1200
3970 BE Driebergen

telefoon
+31 85 401 38 66

website
www.pmpartners.nl

16-7750 mei 2016