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).