Rijksoverheid

Model gegevensbeschermings-effectbeoordeling rijksdienst (PIA)

Model gegevensbeschermings-effectbeoordeling rijksdienst (PIA)

Contact: Ministerie van BZK, directie Constitutionele Zaken en Wetgeving
Pien.Eijnden@minbzk.nl / Lester.Meijenfeldt@minbzk.nl
Ministerie van VenJ, directie Wetgeving en Juridische Zaken
w.m.weeber@minvenj.nl
Functionaris voor gegevensbescherming VenJ en BZK: p.j.de.groot@minvenj.nl

Versie: 1.0
September 2017

Inhoudsopgave

Inleiding

Dit document bestaat uit drie onderdelen. Het eerste deel geeft een algemene inleiding op het instrument gegevensbeschermingseffectbeoordeling – ook wel Privacy Impact Assessment (PIA) – en beschrijft het proces van het uitvoeren van een PIA. Het tweede deel bevat het model om een PIA uit te voeren bestaande uit 17 punten. In het derde deel wordt per punt van het model een toelichting gegeven, uitgesplitst naar een PIA van voorgenomen regelgeving en van door het Rijk voorgenomen gegevensverwerkingen (hierna: overheidsverwerkingen).

Dit model wordt gebruikt in de rijksdienst.[1] Organisaties kunnen dit model voor de eigen organisatie aanvullen met organisatiespecifieke elementen. Door dergelijke elementen toe te voegen, kan het instrument beter toegesneden worden op het eigen organisatieonderdeel en wordt het daarmee beter bruikbaar.

[1] De begrippen Rijk, rijksdienst en overheid worden in dit model door elkaar gebruikt. In alle gevallen wordt bedoeld: het Rijk (kerndepartementen, agentschappen, toezichts- en uitvoeringsorganisaties). Niet onder deze definitie vallen de zelfstandige bestuursorganen, defensie, politie, rechterlijke macht en decentrale overheden. Door een aantal van deze sectoren (o.a. defensie), wordt wel gebruik gemaakt van het Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA).

Deel I - Proceskader

1 Wat is een PIA?

Een PIA is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen.

Dit Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA) vervangt het Toetsmodel Privacy Impact Assessment Rijksdienst van 2013.[2] Dit model is gebaseerd op de nieuwe Europese regelgeving, de Algemene verordening gegevensbescherming (AVG),[3] de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn)[4] en de mede daarop gebaseerde nationale regelgeving. In dit model zijn ook de richtsnoeren van de Europese privacytoezichthouders betrokken.[5] Het model is gericht op de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien en op de verwerking van persoonsgegevens door of in opdracht van een onderdeel van de rijksdienst. Het model is bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen. Dit model PIA rijksdienst is opgenomen in het Integraal Afwegingskader beleid en regelgeving (IAK) en het Handboek Portfoliomanagement Rijk.

Het doel van een PIA is de bescherming van persoonsgegevens onderdeel te maken van het afwegingsproces bij de beleidsvorming. Het instrument is een middel om naleving van de privacyregelgeving te verbeteren.[6] Een PIA is *geen* instrument om vast te stellen of een voorgenomen gegevensverwerking in lijn is met de privacyregelgeving (*compliance*). Met de uitkomsten van een PIA moet wel rekening worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te kunnen tonen dat de privacyregelgeving wordt nageleefd bij het verwerken van persoonsgegevens.

Een PIA kan betrekking hebben op een enkele soort gegevensverwerking. Een PIA kan ook zien op een reeks vergelijkbare verwerkingen die vergelijkbare risico's inhouden.[7] Een PIA hoeft zich dus niet te beperken tot een enkel proces, product of verwerkingsverantwoordelijke, bijvoorbeeld wanneer overheidsorganen een gemeenschappelijke applicatie of verwerkingsomgeving willen opzetten.[8]
Een voltooide PIA bestaat uit een:

A. beschrijving kenmerken gegevensverwerkingen: een beschrijving van de voorgenomen verwerkingen en de verwerkingsdoeleinden;
B. beoordeling rechtmatigheid gegevensverwerkingen: een beoordeling van de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden;
C. beschrijving en beoordeling risico's voor betrokkenen: een beoordeling van de gevolgen en risico's van de voorgenomen verwerkingen voor de rechten en vrijheden van de betrokkenen; en
D. beschrijving voorgenomen maatregelen: de voorgenomen maatregelen om deze gevolgen en risico's van de voorgenomen verwerkingen aan te pakken.[9]

---

2 *Kamerstukken II* 2012/13, 26 643, nr. 282, herdruk 1.

3 Verordening (EU) 679/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)(PbEU 2016, L 119/1).

4 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

5 Richtlijnen van 4 april 2017, WP 248.

6 Overweging 84 AVG.

7 Artikel 35, eerste lid, AVG.

8 Overweging 92 AVG.

9 Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.

2 Waarom een PIA uitvoeren?

Door het uitvoeren van een PIA wordt de bescherming van persoonsgegevens op een gestructureerde manier onderdeel van de belangenafweging en besluitvorming van voorgenomen beleid, regelgeving en (ICT-)projecten binnen de rijksdienst. Dit verhoogt de kwaliteit van de besluitvorming.

Een PIA is in de eerste plaats richtinggevend. Door het model te volgen kunnen relevante privacyrisico's die eerder in de ontwikkeling niet zijn onderkend aan het licht komen. Als dat het geval is, is het noodzakelijk om deze aspecten alsnog in de voorbereiding mee te nemen. Een PIA helpt zo met het identificeren en beheersen van risico's en het vermijden van onnodige kosten (in de zin dat problemen in een later stadium moeten worden opgelost).

Een PIA is ook corrigerend. Tijdens het uitvoeren van de PIA kan blijken dat het nodig is eerdere keuzes te heroverwegen, en vervolgens voor een andere (minder inbreukmakende) oplossing te kiezen om een doelstelling te bereiken. Het kan dus voorkomen dat in een eerder stadium gemaakte keuzes bij nadere beschouwing niet goed genoeg kunnen worden onderbouwd ten opzichte van de hiermee gepaard gaande privacyrisico's. Vanwege het richtinggevende en corrigerende karakter van een PIA kan het uitvoeren ervan een dynamisch proces zijn, waarbij beoogde (beleids)oplossingen of ontwerpen van een systeem geleidelijk worden aangescherpt met als doel de privacyrisico's voor de betrokkenen te verminderen.

Het uitvoeren van een PIA kan zorgen voor vertrouwen in de voorgenomen maatregel, binnen en buiten de organisatie. Het verzamelen van de informatie voor het beantwoorden van de vragen helpt medewerkers en leidinggevenden bij de besluitvorming en het afleggen van verantwoording daarover.
Het uitvoeren van een PIA stimuleert privacybewustwording binnen de rijksdienst.

3 In welke gevallen is een PIA verplicht?

Een PIA moet worden uitgevoerd:
1. bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien;
2. bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.[10]

In de tweede situatie is een PIA dus niet in alle gevallen verplicht voor voorgenomen overheidsverwerkingen, maar alleen bij verwerkingen met een hoog risico. Daarvoor is de AVG leidend.

Een PIA van voorgenomen overheidsverwerkingen is in ieder geval vereist in de volgende gevallen:
a. een systematische en uitgebreide beoordeling van persoonlijke aspecten, die is gebaseerd op geautomatiseerde verwerking, en waarop besluiten worden gebaseerd waaraan rechtsgevolgen zijn verbonden of die de betrokkenen op vergelijkbare wijze wezenlijk treffen;
b. grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;
c. stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten;
d. wanneer de Autoriteit persoonsgegevens heeft geoordeeld dat een PIA verplicht is.[11]

[10] Artikel 35, eerste lid, AVG en artikel 27, eerste lid, Richtlijn.

[11] Artikel 35, derde en vierde lid, AVG en artikel 28, derde lid, Richtlijn.

De Europese privacytoezichthouders hebben in aanvulling hierop criteria opgesteld aan de hand waarvan kan worden beoordeeld of sprake is van een hoog risico.[12] Het gaat hier om verwerkingen waarbij sprake is van:

1. het evalueren en beoordelen van betrokkenen, waaronder profileren en voorspellen;
2. geautomatiseerde besluitvorming met rechtsgevolgen of vergelijkbare gevolgen;
3. systematische observatie, monitoring of controle;
4. verwerking van bijzondere, strafrechtelijke of anderszins gevoelige persoonsgegevens;
5. grote gegevensverwerkingen, gelet op het aantal betrokkenen, de hoeveelheid persoonsgegevens, de duur en geografische reikwijdte van de verwerking;
6. koppelen en combineren van persoonsgegevens;
7. kwetsbare betrokkenen die gegeven de situatie minder in staat zijn om vrijelijk toestemming te geven dan wel op te komen tegen de gegevensverwerking, zoals werknemers, kinderen, verstandelijk beperkten, asielzoekers, ouderen en patiënten;
8. gebruikmaking van nieuwe technologieën;
9. grensoverschrijdend verkeer van persoonsgegevens naar landen buiten de Europese Unie;
10. verhindering van betrokkenen om een recht uit te oefenen of een beroep te doen op een dienst of overeenkomst.

Aan hoe meer criteria de voorgenomen verwerking voldoet, hoe waarschijnlijker sprake is van een hoog risico. De toezichthouders hanteren als vuistregel dat verwerkingen die aan twee of meer van de criteria voldoen, een PIA vereisen.

Als een voorgenomen gegevensverwerking raakt aan grote politiek-bestuurlijke en maatschappelijke vraagstukken is een PIA hoe dan ook gewenst.

Een PIA is in ieder geval *niet* verplicht in de volgende gevallen:[13]

a. de verwerking vindt zijn rechtsgrond in een wettelijke verplichting of een taak van algemeen belang, en in het kader van het vaststellen van deze rechtsgrond is al een PIA verricht.
b. wanneer de Autoriteit persoonsgegevens heeft geoordeeld dat een PIA niet verplicht is.

Volgens de Autoriteit persoonsgegevens hoeft ook geen PIA te worden uitgevoerd wanneer de gegevensverwerking waarschijnlijk geen hoog privacyrisico oplevert of sterk lijkt op een andere gegevensverwerking waarvoor al een PIA is uitgevoerd. Hoewel in het geval onder a een PIA niet verplicht is, kan het toch wenselijk zijn om deze uit te voeren, als in de uitvoering nader invulling wordt gegeven aan zaken die op het niveau van de regelgeving niet aan de orde zijn geweest, bijvoorbeeld de keuze voor een bepaald ICT-systeem en bepaalde beveiligingsmaatregelen.

Indien in strijd met de AVG geen PIA is uitgevoerd of de PIA verkeerd is uitgevoerd, kan de Autoriteit persoonsgegevens een bestuurlijke boete opleggen, tot 10 miljoen euro.[14]

Voor vragen over wanneer een PIA verplicht of wenselijk is, kan contact worden opgenomen met de functionaris voor gegevensbescherming.

4 Hoe verhoudt een PIA zich tot andere instrumenten?

Een PIA wordt gehanteerd naast, en zo nodig in afstemming met andere hulpmiddelen voor ontwikkeling van regelgeving en overheidsverwerkingen. Een PIA komt dus niet in de plaats van andere bestaande instrumenten.

[12] Richtsnoeren van 4 april 2017, WP 248, p. 7-12.

[13] Artikel 35, vijfde en tiende lid, AVG.

[14] Artikel 83, vierde lid, onder a, AVG.

Bij voorgenomen beleid en regelgeving kan daarbij gedacht worden aan instrumenten uit het IAK, zoals:
- de bedrijfseffectentoets (BET);
- de uitvoerbaarheids- en handhaafbaarheidstoets (U&H-toets); en
- toetsing van voorgenomen regelgeving aan hoger recht, waaronder een constitutionele toets.

Bij overheidsverwerkingen kan daarbij gedacht worden aan de volgende normenkaders:
- het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007);
- het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2013 (VIRBI 2013); en
- de Baseline Informatiebeveiliging Rijksdienst 2012 (BIR 2012).

In het kader van informatiebeveiliging volgt uit het VIR 2007 dat voor een informatiesysteem maatregelen op basis van een risicoafweging worden getroffen, met als doel de informatie binnen het systeem adequaat te beveiligen. De genoemde risicoafweging wordt idealiter gemaakt in een risicoanalyse, waarbij de impact van verlies aan informatieveiligheid op het bedrijfsproces wordt bepaald (soms genoemd: *business impact analyse* (BIA)).

Zowel in het VIR 2007 als in de AVG en de Richtlijn wordt gesteld dat de verantwoordelijke een planning- en controlcyclus (plan-do-check-act) heeft ingericht om te borgen dat de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.[15] Het is van belang om eisen van privacy en informatiebeveiliging in samenhang te bezien. Om te voldoen aan de van toepassing zijnde regelgeving zal een verantwoordelijke alle relevante aspecten integraal moeten beschouwen teneinde te borgen dat de uiteindelijk te treffen set van maatregelen in de organisatie en techniek adequaat is. Om redenen van efficiency kan worden overwogen een BIA gelijktijdig met een PIA uit te voeren, alsook de keuze voor de te treffen maatregelen.

5 Wie is verantwoordelijk voor het uitvoeren van een PIA?

Bij beleid en regelgeving
De minister die verantwoordelijk is voor het beleid en de mogelijk daaruit voortvloeiende op te stellen regelgeving is formeel verantwoordelijk voor het uitvoeren van de PIA. In de praktijk ligt die verantwoordelijkheid bij de beleidsdirectie.

Bij overheidsverwerkingen
De verwerkingsverantwoordelijke is verantwoordelijk voor het uitvoeren van een PIA. Formeel is de betreffende minister de verwerkingsverantwoordelijke voor gegevensverwerkingen door een onderdeel van de rijksdienst. In de praktijk zal de bevoegdheid om te beslissen of en op welke wijze persoonsgegevens worden verwerkt zijn gemandateerd, bijvoorbeeld aan een directeur-generaal of een directeur. De gemandateerde functionaris is dan verantwoordelijk voor de uitvoering van een PIA.

Wanneer meerdere ministers verantwoordelijke zijn voor de gegevensverwerkingen, moeten zij gezamenlijk zorgen voor de uitvoering van een PIA.[16] Het ligt in zo'n situatie in de rede dat de minister die het voortouw heeft in de ontwikkeling van het project (denk bijvoorbeeld aan een categoriemanager bij rijksbrede inkoop), het voortouw neemt in het opstellen van de PIA.

Als een onderdeel van de rijksdienst of een organisatie buiten de rijksdienst optreedt als verwerker in de zin van de AVG – dat wil zeggen degene die persoonsgegevens verwerkt namens/in opdracht van een verwerkingsverantwoordelijke – dan is dat onderdeel of die organisatie niet verantwoordelijk voor de PIA. Wel is de verwerker verplicht de verwerkingsverantwoordelijke desgevraagd bijstand te verlenen. Veelal zal de betrokkenheid van de verwerker nodig zijn om de PIA te kunnen uitvoeren.

[15] Artikel 25 AVG en artikel 20 Richtlijn.

[16] Conform artikel 26 AVG en artikel 21 Richtlijn.

6 Wanneer in het proces moet ik een PIA uitvoeren?

Een PIA moet in een vroegtijdig stadium van de beleidsontwikkeling worden uitgevoerd. Op dat moment is het mogelijk om met open vizier na te denken over de effecten en bestaat er nog voldoende gelegenheid om de uitgangspunten van het voorstel zonder grote nadelige consequenties te herzien.
Dit voorkomt ook latere, kostbare aanpassingen in processen, herontwerp van systemen of zelfs stopzetten van een project. Hiermee wordt ook voldaan aan de verplichting uit de privacyregelgeving om bij het ontwerp rekening te houden met gegevensbescherming (*privacy by design*).[17]

Een PIA kan meermaals en op verschillende momenten worden uitgevoerd en geactualiseerd.
Bij wijziging van het voorstel waarmee verwerkingen van persoonsgegevens gemoeid zijn, wordt (opnieuw) een PIA uitgevoerd. In dat geval wordt de wijziging beoordeeld in samenhang met de bestaande verwerkingen. Indien de gegevensverwerkingen (bijvoorbeeld indien meer persoonsgegevens dan voorheen worden verwerkt) of de effecten daarvan veranderen, dient de PIA te worden geactualiseerd. De Europese privacytoezichthouders geven als *good practice* om een PIA elke drie jaar te evalueren (zie ook onder punt 9).

Bij beleid en regelgeving
De PIA moet in ieder geval voorafgaande aan de (internet)consultatie zijn verricht zodat in de consultatie kan worden gereageerd op de uitkomsten van de PIA.

Bij overheidsverwerkingen
De PIA moet in ieder geval zodanig voorafgaand aan de voorgenomen verwerkingen worden verricht dat de uitkomsten van de PIA nog kunnen worden betrokken in de besluitvorming over de voorgenomen verwerkingen.

7 Hoe voer ik een PIA uit?

De uitvoering van een PIA beslaat de volgende processtappen.

1. Verzamel alle relevante informatie over de voorgenomen regelgeving of het projectvoorstel waarbij persoonsgegevens worden verwerkt.

2. Bespreek de punten van het model bij voorkeur in groepsverband, waar diverse relevante expertises deel van uitmaken. Betrokkenheid van meerdere personen met verschillende achtergronden en expertises – denk aan expertise op het gebied van het betreffende beleidsterrein, regelgeving, (informatie)beveiliging en ICT – resulteert in een betere PIA. Voor het uitvoeren van een PIA dient in ieder geval iemand met privacydeskundigheid te worden betrokken. Naast betrokken medewerkers van het betreffende project, kan het wenselijk zijn om iemand van buiten het project te betrekken. De ideale omvang en diversiteit van de groep hangt af van de aard en omvang van de voorgenomen gegevensverwerkingen.

3. Leg de bevindingen schriftelijk vast in een rapport.

4. Consulteer waar passend de personen van wie persoonsgegevens worden verwerkt, de organisaties die hen vertegenwoordigen of andere belanghebbenden.[18] Denk hierbij aan branche- en belangenorganisaties. Het betrekken van belanghebbenden stelt de uitvoerders van de PIA in staat om de zorgen die spelen in kaart te brengen en tegelijkertijd transparant te zijn over de persoonsgegevens die verwerkt zullen gaan worden en de redenen daarvoor. Voor zover persoonsgegevens van eigen personeel worden verwerkt dient de departementale of groepsondernemingsraad te worden

[17] Artikel 25, eerste lid, AVG en artikel 20, eerste lid, Richtlijn.

[18] Artikel 35, negende lid, AVG.

betrokken.[19] Neem in het rapport op wat de geconsulteerden hebben geadviseerd en wat daarmee gedaan is. Indien geen consultatie plaatsvindt, motiveer deze beslissing in het rapport.

Indien de PIA betrekking heeft op een voorstel voor regelgeving, kan consultatie van betrokkenen samenvallen met de bestaande consultatieverplichtingen. Conform het draaiboek voor de regelgeving zal advies over het voorstel worden ingewonnen bij officiële adviescolleges en via internetconsultatie.

5. Leg het PIA-rapport ter advisering voor aan de functionaris voor gegevensbescherming. Neem in het rapport op wat de functionaris heeft geadviseerd en wat daarmee gedaan is. De AVG verplicht tot het inwinnen van advies bij de functionaris voor gegevensbescherming.[20] De Richtlijn wijst enkel op de mogelijkheid en verplicht daar niet als zodanig toe.[21] Het kan verstandig zijn om de functionaris voor gegevensbescherming al eerder in het PIA-proces te betrekken.

6. Indien de gegevensverwerking gepaard gaat met de bouw van een ICT-systeem, moet de departementale Chief Information Officer (CIO) worden betrokken. De CIO toetst het projectplan op duidelijkheid over het verwerken van persoonsgegevens en op argumentatie over de wenselijkheid van het uitvoeren van een PIA. Indien een PIA gewenst is, wordt eveneens getoetst of de uitvoering heeft plaatsgevonden en of de maatregelen in het projectplan zijn opgenomen. Stel de PIA daarom aan de CIO ter beschikking. Indien de PIA wordt uitgevoerd in het kader van ontwikkeling van beleid waarmee 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.

7. Wanneer uit de PIA voor overheidsverwerkingen blijkt dat de verwerking een hoog risico oplevert en de verwerkingsverantwoordelijke er niet in slaagt om maatregelen te nemen om dat (rest)risico te beperken tot een acceptabel niveau, moet de Autoriteit persoonsgegevens voorafgaande aan de voorgenomen verwerking worden geraadpleegd.[22] Als de PIA betrekking heeft op regelgeving moet het voorstel altijd ter consultatie worden toegestuurd aan de Autoriteit persoonsgegevens.[23]
Voor zover de voorgenomen verwerking onder de werkingssfeer van de Richtlijn valt, kan de Autoriteit persoonsgegevens een lijst opstellen van verwerkingen waarbij altijd voorafgaande raadpleging moet plaatsvinden.[24]

   Volgens de Europese privacytoezichthouders is sprake van een onacceptabel hoog (rest)risico wanneer de betrokkene getroffen wordt met significante of onomkeerbare gevolgen die hij mogelijk niet te boven komt of de kans daarop aanzienlijk is.

   Voor het schriftelijk advies van de Autoriteit persoonsgegevens over een voorgenomen verwerking geldt een termijn van acht weken. Die termijn kan naar gelang de complexiteit van de voorgenomen verwerking met zes weken worden verlengd.[25] Neem in het rapport op wat zij heeft geadviseerd en wat daarmee gedaan is.

8. Stuur het definitieve PIA-rapport aan alle betrokkenen bij het opstellen van de PIA, tenzij regels met betrekking geheimhouding daaraan in de weg staan.

---

[19] Artikel 27, eerste lid, onder k en l, Wet op de ondernemingsraden en het Besluit medezeggenschap Defensie 2008.

[20] Artikel 35, tweede lid, AVG. Zie ook Richtlijnen van 13 december 2016 (laatstelijk gewijzigd op 5 april 2017), WP 243, p. 17.

[21] Artikel 34, derde lid, Richtlijn.

[22] Artikel 36, eerste lid, AVG en artikel 28, eerste lid, Richtlijn.

[23] Artikel 36, vierde lid, AVG en artikel 28, tweede lid, Richtlijn.

[24] Artikel 28, derde lid, Richtlijn.

[25] Artikel 36, tweede lid, AVG.

8 Hoe verantwoord ik de uitkomst van een PIA?

De uitkomst van een PIA wordt verantwoord door middel van een rapport volgens het model in deel II.

Bij beleid en regelgeving
Bij regelgeving wordt over PIA-resultaten een passage opgenomen in de memorie of nota van toelichting.[26] Daarin wordt een samenvatting gegeven van de belangrijkste afwegingen en keuzes in de PIA. 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 privacyregelgeving. Hoewel een volledig gestandaardiseerde verantwoordingsparagraaf niet kan worden gegeven, zou een modelelement van deze paragraaf kunnen zijn:

"Gezien de aard van dit voorstel is in de fase van beleidsontwikkeling een gegevensbeschermingseffectbeoordeling uitgevoerd. Met behulp hiervan is de noodzaak onderzocht van de voorgenomen verwerking van persoonsgegevens en zijn op gestructureerde wijze de gevolgen en risico's van de maatregel(en)/het systeem voor gegevensbescherming in kaart gebracht. Hierbij is in het bijzonder aandacht besteed aan de beginselen van transparantie, gegevensminimalisering, doelbinding, het vereiste van een goede beveiliging en de rechten van de betrokkenen. [Beschrijving specifieke aspecten en de in dit geval gemaakte belangenafweging]"

In aansluiting op het beleid over het actief openbaar maken van uitvoerings- en effecttoetsen, moeten de uitkomsten van een PIA – als daarnaar verwezen wordt in de toelichting bij het voorstel – gepubliceerd worden op de voor iedereen toegankelijke wetgevingskalender.[27]

Bij overheidsverwerkingen
De verwerkingsverantwoordelijke moet een register bijhouden van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden.[28] De uitkomsten van de PIA kunnen worden opgenomen in dit register. In het kader van transparantie en draagvlakvergroting kan het wenselijk zijn om (delen van) de uitkomsten van de PIA openbaar te maken, rekening houdend met het afwegingskader van de Wet openbaarheid van bestuur. Zo hoeven bijvoorbeeld kwetsbaarheden van een ICT-systeem niet openbaar gemaakt te worden.

[26] Aanwijzing 212, onder a, Aanwijzingen voor de regelgeving.

[27] *Kamerstukken II* 2016/17, 33 009, nr. 39.

[28] Artikel 30 AVG.

9 Wat moet ik doen nadat de PIA is vastgesteld?

Na vaststelling van de PIA, dient de verwerkingsverantwoordelijke bij de verdere ontwikkeling van de voorgenomen regelgeving of het projectvoorstel rekening te houden met de uitkomsten van de PIA.[29]

De verwerkingsverantwoordelijke beoordeelt indien nodig of de verwerking overeenkomstig de PIA wordt uitgevoerd. Hij doet dat ten minste wanneer sprake is van een verandering van het risico van de verwerkingen.[30] Risico's kunnen veranderen als gevolg van veranderingen in de onderdelen van de verwerkingen (gegevens, middelen, dreigingen etc.), veranderingen in de context (doeleinden, faciliteiten etc.) of veranderingen in de organisatie of de samenleving.

Daarnaast bevelen de Europese privacytoezichthouders als *good practice* aan om een PIA elke 3 jaar opnieuw uit te voeren. De Autoriteit persoonsgegevens noemt het een continu proces. De verantwoordelijke moet (blijven) monitoren of de gegevensverwerkingen wijzigen en of de PIA daarom moet worden bijgesteld.

[29] Overweging 84 AVG.

[30] Artikel 35, elfde lid, AVG.

Deel II - Model

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. **Voorstel**
   Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

2. **Persoonsgegevens**
   Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer.

3. **Gegevensverwerkingen**
   Geef alle voorgenomen gegevensverwerkingen weer.

4. **Verwerkingsdoeleinden**
   Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

5. **Betrokken partijen**
   Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

6. **Belangen bij de gegevensverwerkingen**
   Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

7. **Verwerkingslocaties**
   Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

8. **Technieken en methoden van de gegevensverwerkingen**
   Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of *big data*-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

9. **Juridisch en beleidsmatig kader**
   Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

10. **Bewaartermijnen**
    Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. **Rechtsgrond**
    Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.

15. Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Deel III - Toelichting

Dit deel van de PIA rijksdienst geeft een toelichting op het model van deel II. In deze toelichting worden de relevante bepalingen uit de privacyregelgeving toegelicht. De toelichting is niet opgezet als een handboek privacyregelgeving.

In deze toelichting wordt waar relevant een onderscheid gemaakt tussen een PIA van voorgenomen regelgeving en een PIA van voorgenomen verwerkingen door de overheid. Bij regelgeving gaat het om: wetten, algemene maatregelen van bestuur en ministeriële regelingen. Bij verwerkingen door de overheid gaat het om verwerkingen van persoonsgegevens door of in opdracht van een onderdeel van de rijksdienst. Het object van een PIA kan zijn: een of meerdere producten, diensten, processen of systemen.

Het model bestaat uit 17 punten verspreid over vier onderdelen. Onderdeel A behandelt de feiten van de voorgenomen gegevensverwerkingen. De juridische beoordeling van de feiten komt aan de orde in onderdeel B. Onderdeel C gaat over risico's voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico's aan te pakken. Deze opzet is ontleend aan de privacyregelgeving.[31] Het maken van een PIA is een dynamisch proces. Denkbaar is dat nadat een beoordeling (onder B) is verricht en de risico's (onder C) in kaart zijn gebracht, als maatregel wordt voorgesteld om de voorgenomen verwerkingen zoals beschreven in onderdeel A aan te passen.

De beantwoording van de 17 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de voorgenomen regelgeving of verwerkingen door de overheid. Wel is het in alle gevallen noodzakelijk om alle punten van het model na te gaan en de gemaakte afweging per punt op te schrijven.

A. Beschrijving kenmerken gegevensverwerkingen

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Om een PIA te kunnen verrichten moet duidelijk zijn op welk onderwerp/object deze betrekking heeft. Met een korte en bondige beschrijving van het voorstel waar de PIA op ziet, wordt tevens voorkomen dat bij het nalopen van de 17 punten hier verschillend over wordt gedacht. Ten behoeve van de duidelijkheid kan het nuttig zijn om expliciet aan te geven waar de PIA niet over gaat.

Bij **conceptregelgeving** kan voor deze beschrijving van het voorstel aansluiting worden gezocht bij het voorlopige ontwerp van de inleidende paragraaf van de memorie of nota van toelichting bij het voorstel, voor zover deze betrekking heeft op verwerkingen van persoonsgegevens.

Bij **overheidsverwerkingen** kan in hoofdlijnen worden beschreven hoe de gegevensverwerkingen er uit zullen zien. Als dat er is kan worden aangesloten bij het projectvoorstel of een beschrijving van de architectuur.

[31] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[32] Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven.[33] Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.[34]

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd.[35] Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.[36]

Anonieme en geanonimiseerde gegevens zijn *geen* persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is.[37] Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK-nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

[32] Artikel 4, eerste onderdeel, AVG en artikel 3, eerste onderdeel, Richtlijn.

[33] Overweging 27 AVG.

[34] Overweging 26 AVG en overweging 21 Richtlijn.

[35] Overweging 26 AVG.

[36] Artikel 4, onder vijf, AVG en artikel 3, onder vijf, Richtlijn.

[37] Overweging 26 AVG en overweging 21 Richtlijn.

Bijzondere persoonsgegevens
Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:
- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.[38]

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens
Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon.[39] Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens
Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd.[40] Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.[41]

Gegevens over gezondheid
Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon.[42] Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven.[43] Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

[38] Artikel 9, eerste lid, AVG en artikel 10 van de Richtlijn.

[39] Artikel 4, dertiende onderdeel, AVG en artikel 3, twaalfde onderdeel, Richtlijn.

[40] Artikel 4, veertiende onderdeel, AVG en artikel 3, dertiende onderdeel, Richtlijn.

[41] Overweging 51 AVG.

[42] Artikel 4, vijftiende onderdeel, AVG en artikel 3, veertiende onderdeel, Richtlijn.

[43] Artikel 10 AVG.

Wettelijke identificatienummers
Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIG-nummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens
Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie- en locatiegegevens.[44]

Betrokkenen
Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader.[45] Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd.[46] Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

[44] *Stcrt.* 2013, nr. 5174, p. 14.

[45] Overweging 38 AVG.

[46] Artikel 8, eerste lid, AVG.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
b. personen die voor een strafbaar feit zijn veroordeeld;
c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

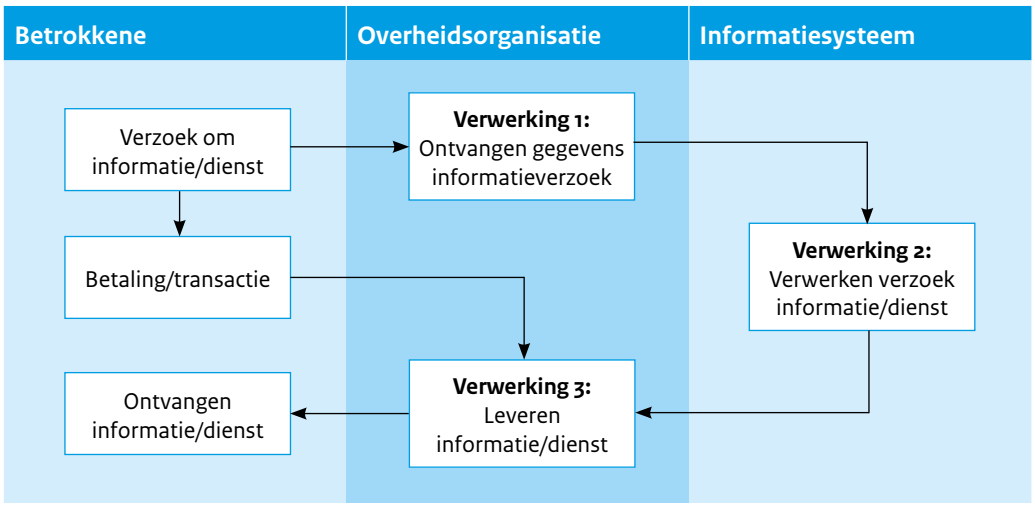
Bij **conceptregelgeving** kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.[47]

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens.[48] Denk hierbij aan: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Indien mogelijk verdient het aanbeveling om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een *input-proces-output* model, *flowchart* of *workflow*.



[47] Artikel 8, eerste lid, Richtlijn.

[48] Artikel 4, tweede onderdeel, AVG en artikel 3, tweede onderdeel, Richtlijn.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld.[49] De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.[50] Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt gedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting.[51] Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

[49] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.

[50] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.

[51] Artikel 6, derde lid, AVG en artikel 8, eerste lid, Richtlijn. Zie ook aanwijzing 162a Aanwijzingen voor de regelgeving.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt.[52] Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.[53]

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[54] De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.[55] Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt.[56] Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

[52] Artikel 4, zevende onderdeel, AVG en artikel 3, onderdeel 8, Richtlijn.

[53] Artikel 26, eerste lid, AVG en artikel 21, eerste lid, Richtlijn.

[54] Artikel 4, achtste onderdeel, AVG en artikel 3, achtste onderdeel, Richtlijn.

[55] Artikel 28, derde lid, AVG en artikel 22, derde lid, Richtlijn.

[56] Artikel 4, negende onderdeel, AVG en artikel 3, tiende lid, Richtlijn.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

6. Belangen bij de gegevensverwerking
Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen tevens de belangen (lees: de waarde of de voordelen) die met de gegevensverwerkingen gemoeid zijn een rol spelen. Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang. Het gaat hier dus niet om de (mogelijk) negatieve gevolgen voor de betrokkenen. Denk hierbij bijvoorbeeld aan: bedrijfsbelangen, financiële belangen en commerciële belangen, het handhaven van juridische vorderingen, toezicht op medewerkers ten behoeve van de veiligheid of managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging, en gezondheid.

Het belang dat gemoeid is met de gegevensverwerkingen werkt door in de toets van de noodzaak (zie punten 11 en 14 hierna).

7. Verwerkingslocaties
Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.[57]

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan.[58] Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit)[59] of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen.[60] Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.[61]

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

[57] Artikelen 55 en 56 AVG en artikel 45 Richtlijn.

[58] Artikel 44 AVG en artikel 35, eerste lid, Richtlijn.

[59] Artikel 45 AVG en artikel 36, Richtlijn.

[60] Artikel 46 AVG en artikel 37 Richtlijn.

[61] Artikel 49 AVG en artikel 38 Richtlijn.

8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en *big data*-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.[62]

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
c. berust op de uitdrukkelijke toestemming van de betrokkene.[63]

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

a. wettelijk is toegestaan; en
b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.[64]

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.[65]

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn**,** geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.[66]

---

[62] Artikel 22, eerste lid, AVG en artikel 11, eerste lid, Richtlijn.

[63] Artikel 22, tweede lid, AVG.

[64] Artikel 11, eerste lid, Richtlijn.

[65] Artikel 4, vierde onderdeel, AVG en artikel 3, vierde onderdeel, Richtlijn.

[66] Artikel 11, derde lid, Richtlijn.

Big data
Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.[67] In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën
Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

9. Juridisch en beleidsmatig kader
Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Voorbeelden van dergelijke wetten zijn: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootsstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet. Deze lijst is niet uitputtend.

Er kan ook departementaal of rijksbreed beleid zijn dat de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de voorgenomen gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

10. Bewaartermijnen
Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is.[68] Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.[69]

[67] Wetenschappelijk Raad voor het Regeringsbeleid (WRR), Big data in een vrije en veilige samenleving, rapport nr. 95, p. 21. De WRR geeft geen scherp omlijnde definitie van big data, maar richt zich op de hoofdkenmerken 1) Data: het gaat om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen, 2) Analyse: de analyse is data gedreven en zoekt geautomatiseerd naar correlaties en 3) gebruik: de analyses moeten leiden tot 'actionable knowledge' (ingrepen in de realiteit op basis van bestandsanalyses).

[68] Artikel 5, eerste lid, onder e, AVG en artikel 4, eerste lid, onder e, Richtlijn.

[69] Artikel 89 AVG en artikel 4, derde lid, Richtlijn.

Bij **conceptregelgeving** zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij **overheidsverwerkingen** moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.[70] Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn.[71] Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.[72] Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

[70] Overweging 39 AVG en overweging 26 Richtlijn.

[71] Met rechtmatigheid wordt gedoeld op rechtmatigheid van de verwerking in de zin van artikel 6 van de AVG en artikel 8 van de Richtlijn. Met rechtmatigheid wordt niet bedoeld volledige *compliance* met de privacyregelgeving.

[72] Artikel 5, eerste lid, onder a, AVG.

e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.[73]

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet.[74] De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.[75]

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.[76]

[73] Artikel 6, eerste lid, AVG.

[74] Artikel 6, derde lid, AVG.

[75] Artikel 8, eerste lid, Richtlijn.

[76] Artikel 4, elfde onderdeel, AVG en overweging 43 AVG.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.[77]

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).[78]

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.[79]

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

a. wettelijk is toegestaan;
b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.[80]

[77] Artikel 9, tweede lid, AVG.

[78] Artikel 10 AVG.

[79] Artikel 10 Wet algemene bepalingen burgerservicenummer.

[80] Artikel 10 Richtlijn.

Bij **conceptregelgeving** kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.[81]

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.[82]

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden.[83] Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.[84]

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
e. het bestaan van passende waarborgen.[85]

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

---

[81] Overweging 52 AVG en overweging 37 Richtlijn.

[82] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.

[83] Artikel 6, vierde lid, AVG jo. artikel 23, eerste lid, AVG.

[84] Artikel 89 AVG.

[85] Artikel 6, vierde lid, AVG.

a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.[86]

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.[87]

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken. Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:
- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij **conceptregelgeving** kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

15. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

[86] artikel 4, tweede lid, Richtlijn.

[87] Artikel 9, eerste lid, Richtlijn.

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen.[88] Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang.[89] Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in **conceptregelgeving** een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden én moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

a. de verwerkingsdoeleinden;
b. de categorieën van persoonsgegevens;
c. het toepassingsgebied van de ingevoerde beperkingen;
d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. de opslagperiodes en de toepasselijke waarborgen;
g. de risico's voor de rechten en vrijheden van betrokkenen;
h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.[90]

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

[88] Hoofdstuk III (artikelen 12-22) AVG en hoofdstuk III (artikelen 12-18) Richtlijn.

[89] Artikel 23 AVG, artikel 13, derde lid, 15 en 16, vierde lid, Richtlijn.

[90] Artikel 23, tweede lid, AVG.

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten.[91] Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico.[92] Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.[93]

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:
1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging.[94] Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren
De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:
- waar de gegevensverwerking kan leiden tot:
  - discriminatie, stigmatisering en uitsluiting;
  - (blootstelling aan) identiteitsdiefstal of -fraude;
  - financiële verliezen;
  - reputatie- of anderszins relationele schade;
  - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
  - ongeoorloofde ongedaanmaking van pseudonimisering;
  - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;

[91] Artikel 35, zevende lid, aanhef en onder c, AVG en artikel 27, tweede lid, Richtlijn.

[92] Overweging 76 AVG.

[93] Overweging 84 AVG.

[94] Artikel 4, aanhef en onder a, van het Besluit voorschrift informatiebeveiliging rijksdienst 2007.

- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.[95]

2. Risico's inschatten
Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens. Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:
- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.[96]

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen. Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen
Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

[95] Overwegingen 75 en 85 AVG en overweging 51 Richtlijn.

[96] Overweging 83 AVG en overweging 60 Richtlijn.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.[97]

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.[98] In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn.[99] Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

a. pseudonimiseren en versleutelen van persoonsgegevens;
b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.[100]

[97] Artikel 5, eerste lid, aanhef en onder f, AVG en artikel 4, eerste lid, onder f, Richtlijn.

[98] Artikel 32 AVG en artikel 29 Richtlijn.

[99] Overwegingen 83 en 94 AVG.

[100] Artikel 32, eerste lid, AVG.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn[101]:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

a. controle op de toegang tot de apparatuur;
b. controle op de gegevensdragers;
c. opslagcontrole;
d. gebruikscontrole
e. controle op de toegang tot gegevens;
f. transmissiecontrole;
g. invoercontrole;
h. transportcontrole; en
i. herstelmogelijkheid.[102]

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.[103]

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

[101] Artikel 5, eerste lid, onder d, AVG en artikel 4, eerste lid, onder d, Richtlijn.

[102] Artikel 29, tweede lid, Richtlijn.

[103] Artikel 25, eerste lid, Richtlijn.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegevens in gebruikte algoritmen en analysemethoden.[104]

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.[105]
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

[104] Kamerstukken II 2016/17, 26 643, nr. 426, p. 7-10.

[105] Artikel 22 AVG.

Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag

September 2017 | 105172