Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Model DPIA Rijksdienst

Inhoud

Voorwoord

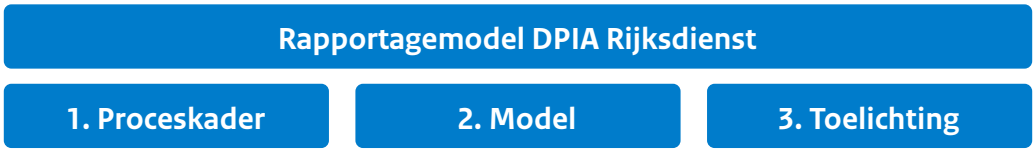
Het Model DPIA Rijksdienst is een model Data Protection Impact Assessment (DPIA) dat binnen de overheid gebruikt wordt om hoog-risico verwerkingen van persoonsgegevens te beoordelen.
Dit document bestaat uit drie onderdelen. Het eerste deel geeft een algemene inleiding op het instrument model DPIA Rijksdienst en beschrijft het proces van het uitvoeren van een DPIA. Het tweede deel bevat het model om een DPIA uit te voeren bestaande uit 17 punten. In het derde deel wordt per punt van het model een toelichting gegeven, uitgesplitst naar een DPIA van regelgeving en gegevensverwerkingen van het Rijk (hierna: gegevensverwerkingen of verwerkingen).

Dit model wordt gebruikt in de Rijksdienst. 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.

Naast het model DPIA Rijksdienst wordt in de Rijksdienst ook gebruikgemaakt van het instrument rapportagemodel DPIA Rijksdienst. Het rapportagemodel wordt gebruikt als sjabloon voor een DPIA-rapportage. Hierin komen de 17 punten naar voren die in het model worden genoemd. De opsteller van een DPIA-rapportage gebruikt het rapportagemodel samen met het model DPIA Rijksdienst om efficiënt een DPIA-rapportage op te stellen.

1. DEEL I – PROCESKADER

Inleiding
Dit document bestaat uit drie onderdelen. Het eerste deel geeft een algemene inleiding op het model DPIA (Data Protection Impact Assessment) en beschrijft het proces van het uitvoeren van een DPIA. Het tweede deel bevat het model om een DPIA uit te voeren bestaande uit 17 punten. In het derde deel wordt per punt van het model een toelichting gegeven met uitgebreide uitleg van definities en voorbeelden ter illustratie. Deze drie onderdelen dienen ter ondersteuning bij het schrijven van het DPIA-rapport met het Rapportagemodel DPIA Rijksdienst.



De bovengenoemde onderdelen vormen tezamen het Rijksmodel DPIA Rijksdienst. Dit model heeft Rijksbrede werking en de documenten zijn gemakkelijk vindbaar via de website van het KCBR.

Verder is ervoor gekozen om Rijksbreed de term DPIA te gebruiken voor het model en de daaruit volgende rapporten in plaats van de termen Privacy Impact Assessment (PIA) en gegevensbeschermings-effectbeoordeling (GEB).

In dit proceskader wordt achtereenvolgens ingegaan op de volgende vragen:
1. Wat is een DPIA?
2. In welke gevallen is een DPIA verplicht?
3. Waarom een DPIA uitvoeren?
4. Wie is verantwoordelijk voor het uitvoeren van een DPIA?
5. Wanneer in het proces moet ik een DPIA uitvoeren?
6. Hoe voer ik een DPIA uit?
7. Hoe verantwoord ik de uitkomst van een DPIA?
8. Hoe verhoudt een DPIA zich tot andere instrumenten?

1.1 Wat is een DPIA?

Een DPIA is een instrument om van projecten, regelgeving en beleid, waarbij persoonsgegevens worden verwerkt, de risico's voor de rechten en vrijheden van betrokkenen in kaart te brengen en te beoordelen in hoeverre de huidige maatregelen voldoen en welke aanvullende maatregelen genomen moeten worden om de risico's zoveel mogelijk te mitigeren. Hoewel een DPIA een verplichting is op basis van de AVG en voornamelijk ziet op het beoordelen van privacyrisico's, dient een DPIA dus breder opgevat te worden.

Het kan gaan om zowel voorgenomen als reeds actieve projecten, regelgeving en beleid. Normaliter wordt een DPIA uitgevoerd, voordat desbetreffende projecten, regelgeving of beleid actief zijn. Echter, hier wordt in de praktijk om uiteenlopende redenen van afgeweken. Daarom wordt in het Model en het Rapportagemodel niet gesproken over voorgenomen gegevensverwerkingen, projecten, regelgeving of beleid, maar is dit op neutrale wijze opgenomen als gegevensverwerking, project, regelgeving of beleid. Dit betekent echter niet dat het juridisch verantwoord is om een DPIA pas te starten of af te ronden als de verwerking van persoonsgegevens al is gestart. Artikel 35 lid 1 van de AVG noemt dat een DPIA uitgevoerd moet worden voordat gestart wordt met de verwerking van persoonsgegevens.

Dit model DPIA is gebaseerd op de Algemene verordening gegevensbescherming (AVG),[1] de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn)[2] en de mede daarop gebaseerde nationale regelgeving, zoals de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). In dit model zijn ook de richtsnoeren van Europees Comité voor gegevensbescherming (EDPB) meegenomen.[3]
Het model is erop gericht om het uitvoeren van een DPIA zo voorspoedig mogelijk te laten verlopen.

Het doel van een DPIA is om bij de verwerking van persoonsgegevens een zo goed en duidelijk mogelijk beeld te hebben wat de risico's zijn bij het verwerken van desbetreffende persoonsgegevens en welke risico mitigerende maatregelen genomen worden om die risico's zoveel mogelijk te mitigeren. Daarnaast is de DPIA zo opgezet dat het beoordelen van deze onderwerpen stapsgewijs en gestructureerd plaatsvindt.

Bij het bepalen van passende maatregelen die genomen dienen te worden om de naleving van de privacyregelgeving aan te tonen, dienen ook de uitkomsten van de DPIA in acht te worden genomen.

Een voltooide DPIA bestaat uit:
A. Beschrijving algemene kenmerken gegevensverwerkingen: een beschrijving van de verwerkingen en de verwerkingsdoeleinden;
B. Beoordeling rechtmatigheid gegevensverwerkingen: een beoordeling en onderbouwing van de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de verwerkingen in relatie tot de verwerkingsdoeleinden;
C. Beschrijving en beoordeling risico's voor betrokkenen: een beoordeling van de gevolgen en risico's van de 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 verwerkingen aan te pakken.[4]

Het wordt ten zeerste aangeraden om het Rapportagemodel DPIA Rijksdienst te gebruiken voor het opstellen van het DPIA-rapport. Door de punten na te lopen die worden benoemd in het rapportage-model en de toelichting uit het Rijksmodel DPIA Rijksdienst te gebruiken, worden in ieder geval alle voor de DPIA noodzakelijke onderwerpen behandeld. Wanneer alle punten van het rapportagemodel zijn behandeld, dan is dat document te gebruiken als finaal DPIA-rapport. Belangrijk om hier aanvullend bij te vermelden is dat het finale document een op zichzelf staand en leesbaar document dient te zijn. Verwijzingen naar documenten waarvan het noodzakelijk is om kennis te nemen bij het lezen van de DPIA dienen als bijlage te worden toegevoegd.

Het Rijksmodel DPIA is niet bedoeld om een verwerking van persoonsgegevens in lijn te brengen met de vereisten uit de Baseline Informatiebeveiliging Overheid (BIO). Het is daarom belangrijk om vooraf of tijdens het schrijfproces van de DPIA contact op te nemen met de departementale (Chief) Information Security Officer (CISO/ISO). Dit geldt uiteraard niet voor DPIA's die zien op wet- en regelgeving.

1.2 In welke gevallen is een DPIA verplicht?

Een DPIA moet worden uitgevoerd:
1. Bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien; of
2. Wanneer sprake is van een verplichting op basis van departementaal beleid; of

[1] 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).
[2] 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.
[3] Richtsnoeren van 4 april 2017, WP 248.
[4] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.

3. Wanneer er gebruik gemaakt wordt van een publieke cloudvoorziening in specifieke omstandigheden, zie voor meer informatie het cloudbeleid[5] ; of
4. Bij gegevensverwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.[6]

Voor het efficiënt uitvoeren van DPIA's op beleidsstukken is een handreiking opgesteld. Deze handreiking zal binnenkort op het Rijksportaal beschikbaar worden gesteld.

Het laatste punt dient te worden beoordeeld aan de hand van de AVG en de DPIA-criteria die zijn opgesteld door de EDPB en de AP zoals hieronder nader toegelicht.

Algemene verordening gegevensbescherming (AVG)
Een DPIA zoals toegelicht onder paragraaf 1.1 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 toezichthoudende autoriteit heeft geoordeeld dat een DPIA verplicht is.[7]

Europees Comité voor gegevensbescherming (European Data Protection Board – EDPB)
De EDPB heeft in aanvulling op bovenstaande punten criteria opgesteld aan de hand waarvan kan worden beoordeeld of sprake is van een hoog risico.[8]

Wanneer aan twee van de criteria wordt voldaan, dan is het waarschijnlijk verplicht om een DPIA uit te voeren. Wanneer aan één van de criteria wordt voldaan, dan moet beoordeeld worden of sprake is van een hoog risico, in welk geval het ook verplicht is om een DPIA uit te voeren. Wanneer wordt besloten geen DPIA uit te voeren, dan dient een beoordeling met onderbouwing schriftelijk plaats te vinden en moet deze worden vastgelegd.

Wanneer een gegevensverwerking raakt aan grote politiek-bestuurlijke en maatschappelijke vraagstukken is een DPIA te allen tijde gewenst.

De meest relevante criteria van de EDPB zijn:
1. Beoordelen van mensen op basis van persoonskenmerken, waaronder profilering en het maken van prognoses, met name op basis van kenmerken als beroepsprestaties, economische situatie of gedrag;
2. Geautomatiseerde besluitvorming, waarbij het gaat om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben;
3. Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht;
4. Verwerking van bijzondere, strafrechtelijke of gevoelige persoonsgegevens;
5. Grootschalige gegevensverwerkingen;
6. Verwerking van persoonsgegevens over kwetsbare personen;

Autoriteit Persoonsgegevens (AP)
Naast de criteria van de EDPB, heeft de AP een lijst van gegevensverwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is.

Hieronder worden de meest relevante criteria van de AP opgesomd.
Deze criteria zijn ook opgenomen in de Pre-Scan DPIA.

[5] Kamerbrief Rijksbreed cloudbeleid 2022 met kenmerk: 2022-0000478290
[6] Artikel 35, eerste lid, AVG en artikel 27, eerste lid, Richtlijn.
[7] Artikel 35, derde en vierde lid, AVG en artikel 28, derde lid, Richtlijn.
[8] Richtsnoeren van 4 april 2017, WP 248, p. 7-12.

- **Heimelijk onderzoek:** persoonsgegevens worden verzameld zonder dat de betrokkene daarvan vooraf op de hoogte wordt gesteld;
- **Zwarte lijsten:** verwerkingen waarbij persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag worden verwerkt;
- **Fraudebestrijding:** de grootschalige verwerking en/of stelselmatige monitoring van (bijzondere) persoonsgegevens voor fraudebestrijding;
- **Financiële situatie:** de grootschalige verwerking en/of stelselmatige monitoring van financiële gegevens;
- **Samenwerkingsverbanden:** het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen (bijzondere) persoonsgegevens uitwisselen;
- **Cameratoezicht:** de grootschalige verwerking en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's;
- **Controle werknemers:** de grootschalige verwerking en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren;
- **Locatiegegevens:** de grootschalige verwerking en/of stelselmatige monitoring van locatiegegevens, bijvoorbeeld met navigatiesystemen en telefoons;
- **Communicatiegegevens:** de grootschalige verwerking en/of stelselmatige monitoring van communicatiegegevens inclusief metadata dat herleidbaar is tot natuurlijke personen;
- **Profilering:** de systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking;
- **Observatie en beïnvloeding van gedrag:** de grootschalige verwerking van persoonsgegevens die op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen observeren of beïnvloeden;
- **Biometrische gegevens:** de grootschalige verwerking en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.

Een DPIA is **niet** verplicht in de volgende gevallen:[9]

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 al een DPIA is verricht;
b. Wanneer de AP heeft geoordeeld dat een DPIA niet verplicht is.
    - Volgens de AP hoeft geen DPIA te worden uitgevoerd wanneer de gegevensverwerking waarschijnlijk geen hoog risico oplevert of sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.

Hoewel in het geval onder (a) een DPIA 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.

Een DPIA kan betrekking hebben op een enkele soort gegevensverwerking.
Een DPIA kan ook zien op een reeks vergelijkbare verwerkingen die vergelijkbare risico's inhouden.[10]
Een DPIA hoeft zich dus niet te beperken tot een enkel proces, product of verwerkingsverantwoordelijke, bijvoorbeeld wanneer overheidsorganen een gemeenschappelijke applicatie of verwerkingsomgeving willen opzetten.[11]

Om te bepalen of een DPIA verplicht is kan gebruik gemaakt wordt van de Pre-scan DPIA of de tool in het register van verwerkingsactiviteiten.

[9] Artikel 35, vijfde en tiende lid, AVG.
[10] Artikel 35, eerste lid, AVG.
[11] Overweging 92 AVG.

Als in strijd met de AVG geen DPIA is uitgevoerd of de DPIA verkeerd is uitgevoerd, kan de AP een bestuurlijke boete opleggen, tot 10 miljoen euro.[12]

Voor vragen over wanneer een DPIA verplicht of wenselijk is, kan contact worden opgenomen met een privacy officer of de functionaris voor gegevensbescherming (FG).

1.3 Waarom een DPIA uitvoeren?

Ook in situaties wanneer het niet verplicht is om een DPIA uit te voeren, kan het waardevol zijn om toch een DPIA uit te voeren. Door het uitvoeren van een DPIA wordt de bescherming van persoonsgegevens namelijk op een gestructureerde manier onderdeel van de belangenafweging en besluitvorming van beleid, regelgeving en (ICT-)projecten binnen de Rijksdienst. Dit verhoogt de kwaliteit van de project- of beleidsuitvoering.

Dit model DPIA is een richtinggevend middel. Door het model te volgen kunnen relevante risico'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 mee te nemen. Een DPIA 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 DPIA kan ook corrigerend werken. Tijdens het uitvoeren van de DPIA 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 worden onderbouwd ten opzichte van de hiermee gepaard gaande risico's.

Vanwege het richtinggevende en corrigerende karakter van een DPIA is het uitvoeren ervan een dynamisch proces, waarbij beoogde (beleids)oplossingen of ontwerpen van een systeem geleidelijk worden aangescherpt met als doel de risico's voor de betrokkenen te verminderen.

Het uitvoeren van een DPIA 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 DPIA stimuleert de privacybewustwording binnen de Rijksdienst.

1.4 Wie is verantwoordelijk voor het uitvoeren van een DPIA?

Bij overheidsverwerkingen
De verwerkingsverantwoordelijke is verantwoordelijk voor het uitvoeren van een DPIA. 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 DPIA.

Wanneer meerdere ministers verantwoordelijke zijn voor een gegevensverwerkingen, moeten zij gezamenlijk zorgen voor de uitvoering van een DPIA.[13] 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), het initiatief neemt in het opstellen van de DPIA.

[12] Artikel 83, vierde lid, onder a, AVG.
[13] Conform artikel 26 AVG en artikel 21 Richtlijn.

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 DPIA. In de praktijk ligt die verantwoordelijkheid bij de beleidsdirectie. De beleidsdirectie is verantwoordelijk voor het aanwijzen van een medewerker of een team van medewerkers om het DPIA-rapport op te stellen.

Verantwoordelijkheid verwerker
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 – is dat onderdeel of die organisatie niet verantwoordelijk voor de DPIA.

Wel is de verwerker verplicht de verwerkingsverantwoordelijke desgevraagd bijstand te verlenen. Veelal zal de betrokkenheid van de verwerker nodig zijn om de DPIA te kunnen uitvoeren.

Zie sectie 3.1.5. voor meer informatie over het onderscheid tussen een verwerker en een verwerkingsverantwoordelijke.

1.5 Wanneer in het proces moet ik een DPIA uitvoeren?

Een DPIA moet in een vroegtijdig stadium van de beleids- of projectontwikkeling worden uitgevoerd. Op dat moment is het namelijk nog 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*).[14]

Een DPIA kan meermaals en op verschillende momenten worden uitgevoerd en geactualiseerd. Bij wijziging van het voorstel waarmee verwerkingen van persoonsgegevens gemoeid zijn, wordt (opnieuw) een DPIA uitgevoerd. In dat geval wordt de wijziging beoordeeld in samenhang met de bestaande verwerkingen. Als de gegevensverwerkingen (bijvoorbeeld indien meer persoonsgegevens dan voorheen worden verwerkt) of de effecten daarvan veranderen, dient de DPIA te worden geactualiseerd. De EDPB stelt als *good practice* om een DPIA iedere drie jaar te evalueren als er geen wijzigingen plaatsvinden in de verwerking. De maatschappij en de technische mogelijkheden die voor handen zijn veranderen tenslotte ook door de jaren heen. Een uitkomst van een dergelijke tussentijdse herziening kan daarom bijvoorbeeld zijn dat bepaalde risico's groter of juist kleiner zijn, of dat er inmiddels betere (minder ingrijpende) alternatieven voor handen zijn om hetzelfde doel te bereiken.

Een DPIA moet dus worden herzien:
- als de verwerking wordt aangepast, waardoor gegevens bijvoorbeeld op een andere manier verwerkt worden, er andere gegevens worden verwerkt of andere partijen betrokken raken bij de verwerking;
- als er 3 jaar lang geen herziening van de DPIA heeft plaatsgevonden.

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

Indien de verwerker via een aanbesteding wordt gecontracteerd betekent dit bijvoorbeeld dat de DPIA voorafgaand aan de aanbesteding wordt uitgevoerd. De uitkomsten van de DPIA kunnen dan worden betrokken bij het opstellen van de offerteaanvraag.

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

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

1.6 Hoe voer ik een DPIA uit?

De uitvoering van een DPIA bestaat in principe uit de volgende processtappen:

1. Verzamel alle relevante informatie over het projectvoorstel, het beleidsvoorstel of de regelgeving waarbij persoonsgegevens worden verwerkt.
   a. Bepaal aan de hand van een Pre-Scan DPIA en/of aan de hand van de criteria uit de AVG, van de AP en de EDPB of een DPIA uitgevoerd moet worden. De Pre-Scan is een drempeltoets voor het uitvoeren van een DPIA. Wanneer de Pre-Scan DPIA ertoe leidt dat geen DPIA uitgevoerd moet worden is het van belang dat de uitgevoerde Pre-Scan gedocumenteerd en gearchiveerd is. Wanneer uit de Pre-Scan komt dat een DPIA moet worden uitgevoerd, dan volgen de volgende processtappen. In het register van verwerkingsactiviteiten is eveneens een tool opgenomen die kan helpen om te bepalen of een DPIA wettelijk is voorgeschreven.
   b. Bepaal wie verwerkingsverantwoordelijke is voor desbetreffende gegevensverwerkingen. De verwerkingsverantwoordelijke(n) is of zijn verantwoordelijk voor het uitvoeren van de DPIA. In deel 3 (toelichting) kan aan de hand van een stroomschema worden bepaald welke organisatie verwerkingsverantwoordelijke(n) is of zijn.
2. Bespreek de punten van het Rapportagemodel DPIA Rijksdienst 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 DPIA. Voor het uitvoeren van een DPIA 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 gegevensverwerkingen.
3. Leg de bevindingen schriftelijk vast in een DPIA-rapport, die wordt opgesteld door middel van het Rapportagemodel DPIA. Voor het schrijven van het DPIA-rapport is het van belang om regelmatig Deel III van het Rijksmodel DPIA te raadplegen; hierin wordt ieder onderwerp dat wordt behandeld in het DPIA-rapport toegelicht met voorbeelden.
4. Consulteer waar passend de personen van wie persoonsgegevens worden verwerkt, de organisaties die hen vertegenwoordigen of andere belanghebbenden.[15] Denk hierbij aan branche- en belangenorganisaties. Het betrekken van belanghebbenden stelt de uitvoerders van de DPIA 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 medewerkers worden verwerkt dient de departementale of groepsondernemingsraad te worden betrokken.[16] Neem in het DPIA-rapport op wat de geconsulteerden hebben geadviseerd en wat daarmee gedaan is. Als geen consultatie plaatsvindt, motiveer deze beslissing in het rapport.
   Als de DPIA 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 DPIA-rapport ter advisering voor aan de FG. Neem in het rapport op wat de FG heeft geadviseerd en wat daarmee gedaan is. Op grond van de AVG is het verplicht om advies in te winnen

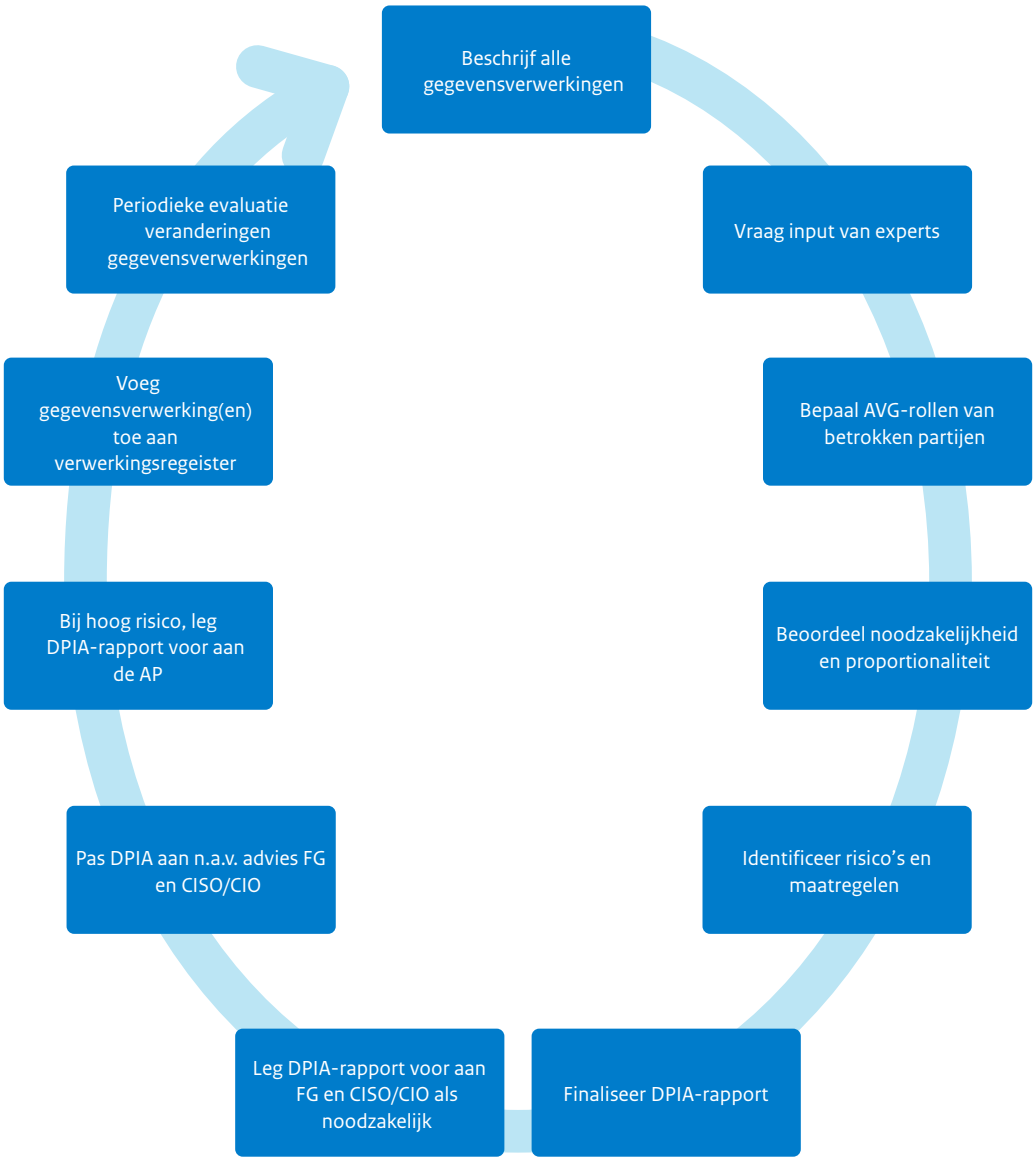
[15] Artikel 35, negende lid, AVG.
[16] Artikel 27, eerste lid, onder k en l, Wet op de ondernemingsraden en het Besluit medezeggenschap Defensie 2008.

bij de FG.[17] Het is ten zeerste aan te raden om de FG zo vroeg mogelijk te betrekken bij de DPIA-procedure en niet te wachten totdat het DPIA-rapport reeds volledig is opgesteld.

6. Als de gegevensverwerking gepaard gaat met de bouw van een ICT-systeem, is het verstandig de departementale Chief Information Officer (CIO) te consulteren. De CIO geeft een oordeel bij de start of tussentijdse wijziging van een project. Onderdeel hiervan is de beoordeling of in het projectplan is opgenomen of sprake is van het verwerken van persoonsgegevens, en of daarbij beargumenteerd is of een DPIA gewenst of noodzakelijk is. Indien de DPIA 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 DPIA voor overheidsverwerkingen blijkt dat de verwerking een hoog risico oplevert en de verwerkingsverantwoordelijke er niet in slaagt om maatregelen te nemen om de resterende risico's te beperken tot een acceptabel niveau, moet de AP voorafgaande aan de verwerking worden geraadpleegd.[18]
   Als de DPIA betrekking heeft op regelgeving moet het voorstel altijd ter consultatie worden toegestuurd aan de AP.[19]
   Voor zover de verwerking onder de werkingssfeer van de Richtlijn valt, kan de AP een lijst opstellen van verwerkingen waarbij altijd voorafgaande raadpleging moet plaatsvinden.[20]
   Volgens de EDPB is in ieder geval 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 AP over een verwerking geldt een termijn van acht weken met een maximale verlenging van zes weken.[21] Neem in het rapport op wat de AP heeft geadviseerd en wat daarmee gedaan is.
   Op basis van artikel 27 Wet op de ondernemingsraden is het ook mogelijk dat de DPIA langs de departementale ondernemingsraad (DOR) of de groepsondernemingsraad Rijk (GOR Rijk) moet. Bijvoorbeeld bij regelingen over het gebruik van personeelsgegevens of voor de inzet van een personeelsvolgsysteem. Hiervoor kan ook Het OR-privacyboekje van de Autoriteit Persoonsgegevens geraadpleegd worden.
8. Stuur het definitieve DPIA-rapport aan alle betrokkenen bij het opstellen van de DPIA, tenzij regels met betrekking tot geheimhouding in de weg staan.
9. Voeg de DPIA en de gegevensverwerkingen die zijn beoordeeld in de DPIA toe aan het register van verwerkingsactiviteiten. Wanneer binnen de content van de DPIA sprake is van een (zelflerend) algoritme, dan dient dit algoritme opgenomen te worden in het algoritmeregister.
10. Evalueer periodiek (in ieder geval iedere drie jaar) of de gegevensverwerkingen binnen de DPIA zijn gewijzigd en hoe significant deze wijzigingen zijn. Bij wijzigingen die negatieve invloed hebben op de rechten en vrijheden van de betrokkenen, dan moet de DPIA worden herzien, een bijlage met de nieuwe gegevensverwerkingen worden toegevoegd of een nieuwe DPIA worden uitgevoerd.
11. Wanneer persoonsgegevens worden doorgegeven aan een andere zelfstandige verwerkingsverantwoordelijke (derde) binnen de scope van de DPIA, dan is het aan te raden om toe te lichten wat deze derde met de gegevens doet. Op die manier kan de verwerking in bredere context beoordeeld worden.
    Daarnaast is het aan te raden om na te gaan of de verwerkingen die door de derde wordt verricht binnen de kaders van de geldende privacywetgeving plaatsvinden. Hoewel dit dus niet binnen de verwerkingsverantwoordelijkheid van het Rijksonderdeel dat de DPIA uitvoert valt, is het wel wenselijk om een volledig beeld te schetsen van de verwerking, inclusief eventuele verwerkingen verricht door een derde partij. Dit kan ook door een DPIA die door deze derde is uitgevoerd bij de DPIA te voegen of hiernaar te verwijzen (als deze via een publieke bron te raadplegen is). Indien persoonsgegevens worden doorgegeven aan een derde partij die kwalificeert als een zelfstandige verwerkingsverantwoordelijke dan moet daar een rechtsgrondslag voor bestaan.

[17] Artikel 35, tweede lid, AVG. Zie ook Richtsnoeren van 13 december 2016, WP 243, p. 17.
[18] Artikel 36, eerste lid, AVG en artikel 28, eerste lid, Richtlijn.
[19] Artikel 36, vierde lid, AVG en artikel 28, tweede lid, Richtlijn.
[20] Artikel 28, derde lid, Richtlijn.
[21] Artikel 36, tweede lid, AVG.

Processtappen uitvoering DPIA

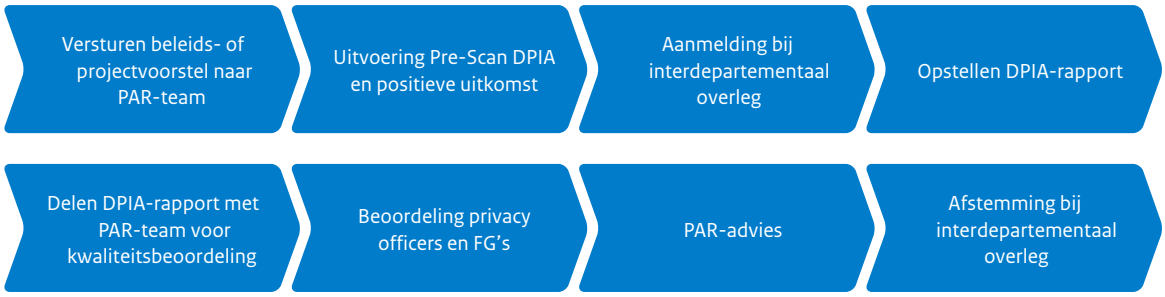


Proces bij Rijksbrede bedrijfsvoeringstrajecten
Wanneer de DPIA een Rijksbreed bedrijfsvoeringstraject betreft, dan dient de PAR-procedure doorlopen te worden.

PAR staat voor Privacy Adviseur Rijk en is onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Rijksbreed betekent in dit kader dat sprake is van de betrokkenheid van ten minste 6 departementen. Wanneer de DPIA een project betreft waarbij minder dan 6 departementen betrokken zijn, dan hoeft de PAR-procedure niet doorlopen te worden.

Hieronder is de PAR-procedure in het kort beschreven. Neem contact op met het PAR-team voor meer informatie.

1. Met het PAR-team wordt een Pre-Scan DPIA doorlopen ter beoordeling of een DPIA uitgevoerd moet worden die door de PAR-procedure moet.
2. Na afronding van het DPIA-rapport wordt deze gedeeld met het PAR-team. Hier wordt een eerste kwaliteitsbeoordeling gedaan.
3. Wanneer de kwaliteitsbeoordeling succesvol is, dan wordt het DPIA-rapport ter beoordeling gestuurd naar de privacy officers en vervolgens naar de functionarissen gegevensbescherming.
4. Nadat de beoordelingen van de privacy officers en de FG's binnen zijn, wordt een PAR-advies geschreven.
5. De projectleider dient vervolgens het DPIA-rapport af te stemmen bij een interdepartementaal overleg, zoals het GOR-rijk.



1.7 Hoe verantwoord ik de uitkomst van een DPIA?

Het doel van de DPIA en het daaruit volgende rapport is dat hiermee kan worden voldaan aan de verantwoordingsplicht wat betreft het uitvoeren van de gegevensverwerkingen.

Door het Rapportagemodel DPIA Rijksdienst samen te gebruiken met Deel II (model) en Deel III (toelichting) van het Model DPIA Rijksdienst, wordt deze verantwoording op gestructureerde wijze gedocumenteerd.

Bij overheidsverwerkingen
De verwerkingsverantwoordelijke moet een register bijhouden van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden.[22] De uitkomsten van de DPIA kunnen worden opgenomen in dit register. In het kader van transparantie en draagvlakvergroting kan het wenselijk zijn om (delen van) de uitkomsten van de DPIA 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.

[22] Artikel 30 AVG.

Bij beleid en regelgeving
Bij regelgeving wordt over DPIA-resultaten een passage opgenomen in de memorie of nota van toelichting.[23] Daarin wordt een samenvatting gegeven van de belangrijkste afwegingen en keuzes in de DPIA. 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 DPIA uitgevoerd. Met behulp hiervan is de noodzaak onderzocht van de 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 DPIA – als daarnaar verwezen wordt in de toelichting bij het voorstel – gepubliceerd worden op de voor iedereen toegankelijke wetgevingskalender.[24]

1.8 Hoe verhoudt een DPIA zich tot andere instrumenten?

Een DPIA wordt gehanteerd naast, en zo nodig in afstemming met andere hulpmiddelen voor ontwikkeling van regelgeving en overheidsverwerkingen. Een DPIA komt dus niet in de plaats van andere bestaande instrumenten. Naast de DPIA moeten ook andere instrumenten worden uitgewerkt voor de gegevensverwerkingen gestart mogen worden.

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

Bij overheidsverwerkingen kan bijvoorbeeld 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 Overheid (BIO).

Afhankelijk van de situatie, is het raadzaam en soms verplicht, om naast de hierboven genoemde kaders en voorschriften gebruik te maken van de volgende middelen en voorschriften:

Data transfer impact assessment:
Als persoonsgegevens doorgegeven worden naar een land buiten de Europese Economische Ruimte en het gebruikte doorgiftemechanisme op basis van artikel 46 AVG niet gebaseerd is op een adequaatheidsbesluit (bijvoorbeeld als gebruik gemaakt wordt van standard contractual clauses (SCCs)), is het noodzakelijk om een zogenoemde data transfer impact assessment (DTIA) uit te voeren. Neem contact op met een privacy officer, privacy jurist of de functionaris gegevensbescherming (FG) om na te gaan of deze verplichting van toepassing is. Het is aan te raden om de DTIA als bijlage op te nemen bij de DPIA en de genomen aanvullende technische maatregelen op te nemen bij vraag 17. Momenteel is de Werkgroep DTIA bezig met de selectie van een model DTIA.

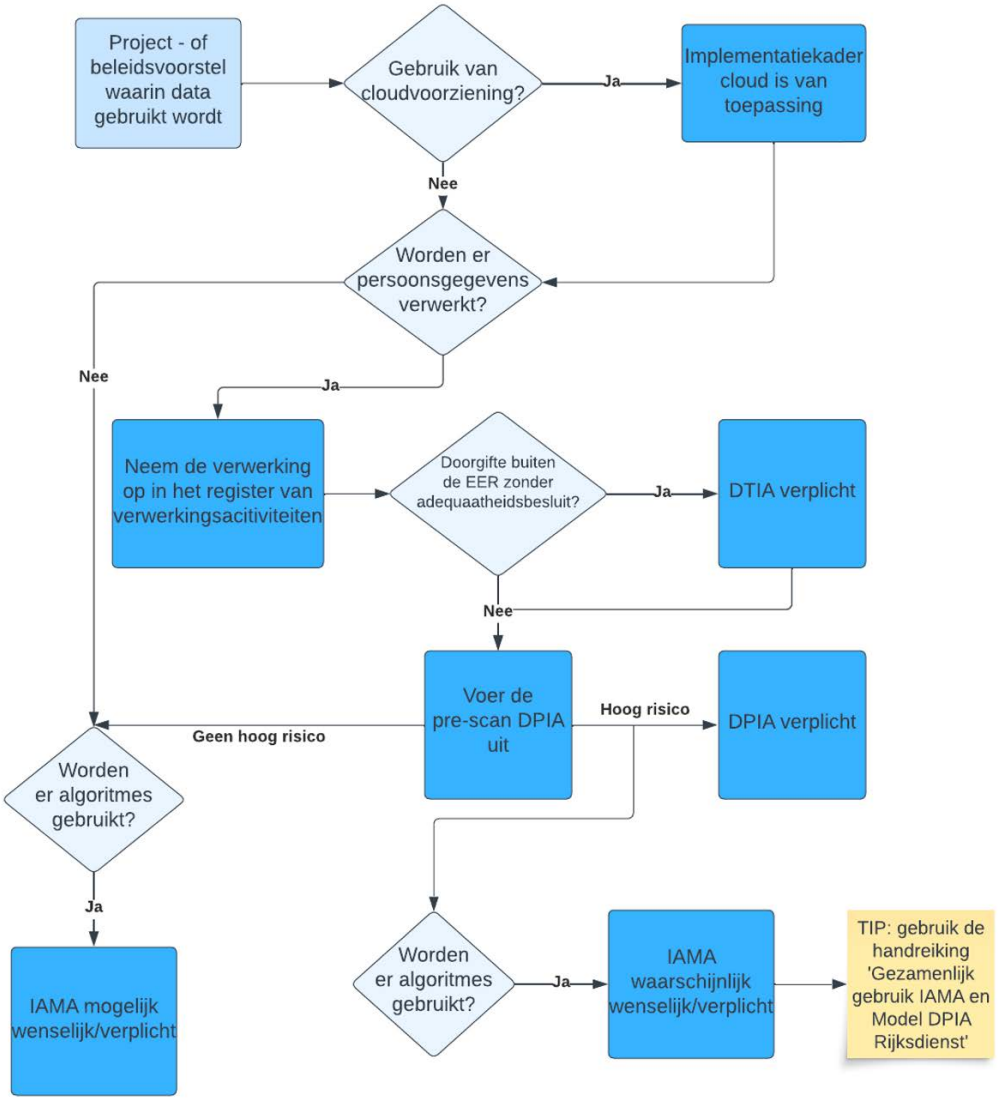
[23] Aanwijzing 212, onder a, Aanwijzingen voor de regelgeving.
[24] *Kamerstukken II* 2016/17, 33 009, nr. 39.

Impact Assessment Mensenrechten en Algoritmes
Als gebruik gemaakt wordt van algoritmes is het aan te raden, en afhankelijk van de situatie zelfs verplicht, om een Impact Assessment Mensenrechten en Algoritmes (IAMA) uit te voeren. Het IAMA kan met behulp van de handreiking 'gezamenlijk gebruik IAMA en Model DPIA Rijksdienst' efficiënt gelijktijdig met de DPIA worden uitgevoerd. Deze handreiking zal via het Rijksportaal beschikbaar worden gesteld.

Rijksbreed cloudbeleid 2022
Indien gegevens opgeslagen of anderszins verwerkt worden in een publieke cloudvoorziening is daarop het cloudbeleid en het implementatiekader 'risicoafweging cloudgebruik' van toepassing.

Het is belangrijk dat voldaan wordt aan alle normenkaders en alle aanvullende modellen volledig zijn ingevuld voordat de DPIA definitief wordt vastgesteld en voor besluitvorming wordt aangeboden. Een goede DPIA bevat een verwijzing naar de relevante normenkaders en voorschriften en de manier waarop daar invulling aan gegeven is, zoals een advies van de CISO van het betreffende departement waarin hij of zij akkoord geeft op de naleving van de BIO en de technische en organisatorische maatregelen die omschreven worden bij vraag 17.

Hieronder volgt een stroomschema met de bovengenoemde tools en instrumenten:



2. DEEL II – MODEL DPIA RIJKSDIENST

Dit model bestaat uit 17 punten verspreid over vier onderdelen. Onderdeel A behandelt de feiten van de gegevensverwerkingen. Onderdeel B beoordeelt de rechtmatigheid van de behandelde feiten uit onderdeel A. 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.[25]

Het maken van een DPIA is een dynamisch proces. Het is aannemelijk dat bij het beoordelen van de risico's onder C en de maatregelen onder D, dat de gegevensverwerkingen in de praktijk gewijzigd dienen te worden, bijvoorbeeld omdat de beoordeelde risico's toch te groot blijken te zijn op basis van de huidige gegevensverwerkingen. Wanneer de gegevensverwerkingen in de praktijk zijn gewijzigd, dan dienen de punten uit onderdeel A en B ook gewijzigd te worden om de realiteit te reflecteren.

De beantwoording van de 17 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de 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 afwegingen per punt op te schrijven.

A. Beschrijving algemene kenmerken gegevensverwerkingen

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

1. **Voorstel**
   Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

2. **Persoonsgegevens**
   Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

3. **Gegevensverwerkingen**
   Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevens-verwerkingen worden toegevoegd.

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

5. **Verwerkingsdoeleinden**
   Beschrijf de doeleinden van alle gegevensverwerkingen.

[25] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn (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 persoons-gegevens 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.)

6. **Betrokken partijen**
   Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens.

7. **Belangen bij de gegevensverwerkingen**
   Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen.
   Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

8. **Verwerkingslocaties**
   Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn.

9. **Juridisch en beleidsmatig kader**
   Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn[26] hoeven niet genoemd te worden.

10. **Bewaartermijnen**
    Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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

11. **Rechtsgrond**
    Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan.

12. **Bijzondere persoonsgegevens**
    Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is.
    Bij verwerking van een wettelijk identificatienummer, beoordeel of dit is toegestaan.

13. **Doelbinding**
    Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

14. **Noodzaak en evenredigheid**
    Beoordeel of de gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op:
    a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

[26] Richtlijn gegevensbescherming opsporing en vervolging.

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

15. Rechten van de betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, beschrijf 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 gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerkingen.

16. Risico's voor betrokkenen

Beschrijf en beoordeel alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen, zoals het recht op privacy en het verbod op discriminatie. Ga in ieder geval in op:

a. Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
b. De oorsprong van deze gevolgen;
c. De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden; en
d. De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Beoordeel per geïdentificeerd risico wat het risiconiveau is op basis van de formule kans x impact. Gebruik hiervoor de niveaus laag, gemiddeld en hoog.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de 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. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

3. DEEL III – TOELICHTING

Dit deel van de DPIA geeft een toelichting op het model van deel II. De toelichting dient gebruikt te worden naast het Rapportagemodel DPIA; bij ieder punt wordt uitgebreid toegelicht wat wordt bedoeld, wat wordt verwacht qua beschrijving en worden voorbeelden gegeven ter illustratie.

In deze toelichting wordt, waar relevant, een onderscheid gemaakt tussen een DPIA van regelgeving en een DPIA van 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 DPIA kan zijn: een of meerdere producten, diensten, processen of systemen.

A. Beschrijving algemene kenmerken gegevensverwerkingen

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

3.1 Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Er moet een DPIA worden uitgevoerd, omdat de verwerking van persoonsgegevens risico's met zich meebrengt die impact hebben op de rechten en vrijheden van de betrokkenen. In geval van beleid en regelgeving moet een DPIA worden uitgevoerd als die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien.

De DPIA heeft als doel deze risico's te identificeren en zoveel mogelijk te verminderen (mitigeren). Echter, voor de uitvoering van een legitieme DPIA moet duidelijk zijn op welke verwerkingen van persoonsgegevens deze betrekking hebben (gegevensverwerkingen).

Met een korte en bondige beschrijving van de gegevensverwerkingen, wordt de reikwijdte van het DPIA-rapport duidelijk en wordt voorkomen dat bij het nalopen van de 17 punten verschillend wordt gedacht. Ten behoeve van de duidelijkheid en de reikwijdte kan het ook nuttig zijn om expliciet aan te geven waar de DPIA in ieder geval niet over gaat.

Ter controle of de beschrijving van het voorstel compleet is kunnen de volgende punten worden nagegaan:
1. Wat is de aanleiding voor het voorstel;
2. Vervangt of vernieuwt het voorstel een bestaande situatie en is deze bestaande situatie beschreven in relatie tot de nieuwe situatie;
3. Welke departementen en organisaties zijn betrokken bij het voorstel;
4. Is bij het voorstel sprake van *privacy by design* en *privacy by default* en is beschreven hoe deze beginselen geïmplementeerd zijn; en
5. Wat zijn de redenen dat het voorstel op deze manier tot stand is gekomen en wordt uitgevoerd?

Privacy by Design
Privacy by design, ook wel gegevensbescherming door ontwerp genoemd, houdt in dat privacy en gegevensbescherming mee worden genomen als eisen bij de ontwikkeling van nieuw beleid en/of nieuwe gegevensverwerking. Dit beginsel is een verplichting voor de verwerkingsverantwoordelijke.

In beginsel moet een zo klein mogelijke inbreuk op de privacy van betrokkenen plaatsvinden bij gegevensverwerkingen.

Welke praktische maatregelen kunnen worden genomen om invulling te geven aan privacy by design? Om dit te bepalen kan rekening worden gehouden met de volgende elementen:
- De stand van de techniek die van toepassing is in het verwerkingsproces;
- De uitvoeringskosten;
- De aard, omvang, context en het doel van de verwerking; en
- De risico's voor de betrokkene

Deze elementen bepalen samen welke technische en organisatorische maatregelen genomen moeten worden om de nodige privacybeschermende waarborgen vanaf het begin van het verwerkingsproces in te bouwen.

Privacy by default
Privacy by default, ook wel gegevensbescherming door standaardinstellingen genoemd, houdt in dat bij de ontwikkeling van nieuw beleid en/of nieuwe verwerkingsprocessen alle instellingen, opties en functies zijn ingesteld op de meest privacy vriendelijk mogelijke manier.

Voorbeelden hiervan zijn:
- Bij het plaatsen van cookies is standaard geselecteerd dat alleen de noodzakelijke cookies worden geplaatst;
- Wanneer alleen een e-mailadres nodig is voor het doeleinde van de gegevensverwerking, vraag niet andere gegevens dan het e-mailadres;
- Bij het mogelijk maken van het delen van digitale mappen met medewerkers, stel als standaard in dat deze mappen alleen toegankelijk zijn voor specifieke medewerkers en niet voor iedereen toegankelijk is.

Zowel het beginsel *privacy by design* als *privacy by default* worden in overweging 78 van de AVG genoemd als verplichting om meegenomen te worden bij openbare aanbestedingen.

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

Bij een overheidsverwerking 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.

3.2 Persoonsgegevens

Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

Betrokkenen: personen waarop de gegevens betrekking hebben
Betrokkenen zijn alle geïdentificeerde of identificeerbare natuurlijke personen binnen de gegevensverwerkingen, oftewel de personen over wie de persoonsgegevens worden verwerkt. Denk hierbij aan:
- Medewerkers,
- Consumenten,
- Cliënten,
- Patiënten,
- Zakelijke contacten,
- Bezoekers,

- Gebruikers,
- Ingezetenen van een gemeente.

Kwetsbare groepen
De categorieën 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 betrokkenen of omdat er een machtsverhouding bestaat tussen de verwerkingsverantwoordelijke en de betrokkene.

Denk bijvoorbeeld aan:
- Minderjarigen,
- Ouderen,
- Verstandelijk gehandicapten,
- Medewerkers,
- 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,
- Asielzoekers,
- Etnische minderheden.

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.[27] Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden, 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, als de toestemming of machtiging tot toestemming wordt verleend door de wettelijke vertegenwoordiger van het kind (bv. Ouder of voogd).[28] Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop het kind geïnformeerd moet worden; de uitleg moet aangepast worden zodat het kind de gegevensverwerking kan begrijpen.

Richtlijn politiële en justitiële gegevens
De Europese Richtlijn beschermen personen bij de verwerking van hun persoonsgegevens die verband houden met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten en de tenuitvoerlegging van straffen. Deze Richtlijn is sinds 2016 van toepassing en verbetert, onder meer, de gegevensuitwisseling tussen handhavingsautoriteiten, zoals de politie, en biedt een betere bescherming van de rechten van betrokkenen. De Nederlandse wetgever heeft deze Richtlijn geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

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.

[27] Overweging 38 AVG.
[28] Artikel 8, eerste lid, AVG.

Definitie persoonsgegevens
Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[29] De term 'natuurlijke personen' betekent hier levende mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in principe geen persoonsgegeven.[30]

Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, waaronder selectietechnieken.[31]

Hieronder staan voorbeelden van *categorieën* persoonsgegevens en *type* persoonsgegevens die binnen die categorie vallen:
- **Naam** (voornaam, achternaam, voorvoegsel, initialen)
- **Contactgegevens** (huisadres, telefoonnummer, e-mailadres)
- **Demografische gegevens** (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
- **Apparaat- en internetgegevens** (IP-adres, MAC-adres, metadata*, locatie-informatie, geografische informatie**, loggegevens)
- **Financiële gegevens** (bankrekeningnummer en -saldo, inkomens- en vermogensgegevens, loonschaal, kredietwaardigheid, winst eenmanszaak)
- **Werk gerelateerde gegevens** (KvK-nummer, zakelijk e-mailadres, verslag van een functioneringsgesprek, documentatie over negatief gedrag op de werkvloer)
- **Support/helpdeskgegevens** (klant – of personeelsnummer, gestelde vraag, opname gesprek)
- **Overige persoonsgegevens** (voertuigidentificatienummer, persoonlijke voorkeuren)

* Ook metadata zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Over het algemeen is een type metadata op zichzelf niet voldoende identificerend, maar meestal worden meerdere type metadata verzameld van gebruikers. Al deze gegevens gecombineerd met elkaar kan leiden tot identificeerbaarheid van een individu. Voorbeelden van metadata zijn:

welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt, wanneer is ingelogd, hoelang de gebruiker ingelogd is gebleven, welke webpagina's zijn aangeklikt 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.

Pseudonieme persoonsgegevens
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 aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.[32]

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden ook als persoonsgegevens beschouwd.[33] Deze gegevens kunnen namelijk met gebruik van een sleutel weer teruggeleid worden tot een gegeven waarmee een persoon geïdentificeerd kan worden.

[29] Artikel 4, eerste onderdeel, AVG en artikel 3, eerste onderdeel, Richtlijn (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.)
[30] Overweging 27 AVG.
[31] Overweging 26 AVG en overweging 21 Richtlijn.
[32] Artikel 4, onder vijf, AVG en artikel 3, onder vijf, Richtlijn.
[33] Overweging 26 AVG.

Anonieme gegevens
Anonieme en geanonimiseerde gegevens zijn *geen* persoonsgegevens. Relevante privacy wet- en regelgeving zijn niet van toepassing op deze gegevens.

Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie de persoonsgegevens betrekking hebben, niet (meer) identificeerbaar is.[34] Let op: het anonimiseren van persoonsgegevens als handeling is een verwerking van persoonsgegevens en valt *wel* onder privacy wet- en regelgeving.

Gevoelige persoonsgegevens
Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens betekent niet dat geen sprake is van een hoog risico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog risico met zich meebrengen. Daarom wordt de categorie gevoelige persoonsgegevens hier onderscheiden, ondanks het feit dat deze categorie niet in de AVG voorkomt.

Voorbeelden van gevoelige persoonsgegevens zijn:
- Gegevens over de financiële situatie van de betrokkene;
- (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.[35]

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn persoonsgegevens die in principe verboden zijn om te verwerken.

Om bijzondere persoonsgegevens toch rechtmatig te verwerken moet een uitzonderingsgrond uit de AVG van toepassing zijn.

In de AVG is een limitatieve opsomming opgenomen van deze 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.[36]

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers en de ledenlijst van een politieke partij.

Beeldmateriaal
Uit beeldmateriaal zoals foto's en camerabeelden kunnen bijzondere persoonsgegevens, zoals etnische afkomst, religieuze overtuiging of medische gesteldheid, worden afgeleid. Echter, bij beeldmateriaal is pas sprake van de verwerking van bijzondere persoonsgegevens wanneer de verwerking van het beeldmateriaal het doel heeft om onderscheid te maken met die bijzondere persoonsgegevens. Wanneer het doel van de verwerking niet is gericht op het maken van onderscheid op basis van die bijzondere persoonsgegevens, dan wordt verondersteld dat geen bijzondere persoonsgegevens worden verwerkt.

[34] Overweging 26 AVG en overweging 21 Richtlijn.
[35] *Stcrt.* 2013, nr. 5174, 'CBP Richtsnoeren: Beveiliging van persoonsgegevens', p. 14.
[36] Artikel 9, eerste lid, AVG en artikel 10 van de Richtlijn.

Genetische gegevens
Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over de fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon.[37] 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.[38]
Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, looppatroon en stemgeluid. Foto's (en andere gegevens die hierboven zijn genoemd) 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.[39] Neem bij twijfel altijd contact op met een privacy officer.

Gegevens over gezondheid
Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon.[40] Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Nationaliteit en ras/etnische afkomst
Het gegeven 'nationaliteit' op zichzelf is geen bijzonder persoonsgegeven en wordt ook niet zo genoemd in de AVG en de UAVG als zodanig. Echter, een persoonsgegeven is niet alleen bijzonder wanneer het direct het desbetreffende bijzondere persoonsgegeven onthult. Ook gegevens die indirect dergelijke informatie onthullen, dienen aangemerkt te worden als bijzondere categorieën van persoonsgegevens.[41]

Wanneer het gegeven 'nationaliteit' wordt verwerkt in combinatie met gegevens als geboorteland, geboorteplaats, herkomst en/of pasfoto, dan blijkt uit rechtspraak dat deze gegevens gecombineerd wel leiden tot gegevens waaruit het ras of etnische afkomst blijkt.[42] Echter, volgens de AP is pas sprake van het verwerken van bijzondere persoonsgegevens wanneer het verwerken van het gegeven 'nationaliteit' tot doel heeft om onderscheid te maken naar ras of etnische afkomst, of indien het voor de verwerkingsverantwoordelijke redelijkerwijs voorzienbaar is dat de verwerking tot het maken van onderscheid naar ras of etnische afkomst zal leiden.[43]

Het gebruik van nationaliteit kan wel leiden tot de beoordeling dat het een gevoelig persoonsgegeven is, zoals in het kader van fraudebestrijding en het gebruiken van nationaliteit als indicator van fraude.[44] Daarom is het voor de beoordeling van ieder verwerkt persoonsgegeven zeer van belang om vast te stellen wat het doeleinde is van de verwerking van desbetreffende persoonsgegeven. Ook moet worden beoordeeld of in desbetreffende gegevensverwerking het neutrale gegeven 'nationaliteit' potentieel kan leiden tot discriminatie van de betrokkene en welke andere mogelijke risico's de verwerking heeft voor de betrokkene.

[37] Artikel 4, dertiende onderdeel, AVG en artikel 3, twaalfde onderdeel, Richtlijn.
[38] Artikel 4, veertiende onderdeel, AVG en artikel 3, dertiende onderdeel, Richtlijn.
[39] Overweging 51 AVG.
[40] Artikel 4, vijftiende onderdeel, AVG en artikel 3, veertiende onderdeel, Richtlijn.
[41] Kamerstukken II 2017/18, 34851, nr. 3, p. 40.
[42] Vergelijk overweging 5 van de uitspraak van de rechtbank Rotterdam van 16 mei 2012 (ECLI:NL:RBROT:2012:BW5513), overweging 4.1 van de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 13 augustus 2014 (ECLI:NL:RVS:2014:3002) en overweging 13 tot en met 16 van de uitspraak van de rechtbank Rotterdam van 11 september 2018 (ECLI:NL:RBMNE:2018:4404). Deze overige verwerkte gegevens zijn bijvoorbeeld: geboorteland, geboorteplaats, herkomst en/of pasfoto.
[43] Autoriteit Persoonsgegevens, 'Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag', Onderzoeksrapport z2018-22445, p. 35.
[44] Kamerstukken II, 35 510, nr. 2, Parlementaire ondervragingscommissie Kinderopvangtoeslag, 'Ongekend Onrecht. Verslag - Parlementaire ondervragingscommissie Kinderopvangtoeslag', 17-12-2020.

Strafrechtelijke persoonsgegevens
Strafrechtelijke persoonsgegevens zijn persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.[45] Verder worden ook persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag als strafrechtelijke persoonsgegevens beschouwd.[46] Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Meer in het algemeen, gaat het om persoonsgegevens die betrekking hebben op gedragingen die aanleiding geven tot maatschappelijke afkeuring en de bescherming van deze persoonsgegevens heeft als doel om te voorkomen dat betrokkenen gestigmatiseerd worden of op andere manier ernstige wijze inbreuk wordt gemaakt op hun privé- of beroepsleven.[47]

Volgens rechtspraak van het Europese Hof van Justitie zijn er drie criteria relevant om te beoordelen of sprake is van strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG:
- Juridische kwalificatie van het strafbare feit naar nationaal recht;
- Aard van het strafbare feit; en
- De zwaarte van de sanctie die aan de betrokkene kan worden opgelegd.

Zelfs voor strafbare feiten die naar nationaal recht niet als strafbare feiten in strafrechtelijke zin worden gekwalificeerd, kan uit de aard van het strafbare feit zelf en/of uit de zwaarte voortvloeien dat sprake is van strafrechtelijke persoonsgegevens.[48]

Voorbeelden van strafrechtelijke persoonsgegevens zijn:
- Proces-verbaal,
- Sepotbeslissing,
- Strafblad, relaas verhoor en
- Aanvraag voor een toevoeging in een strafzaak.

Strafrechtelijke persoonsgegevens kunnen, bijvoorbeeld, ook voorkomen in zwarte lijsten en een Verklaring Omtrent Gedrag (VOG). Dat is niet per definitie het geval, omdat een zwarte lijst ook kan bestaan uit negatieve gegevens over personen die niet strafrechtelijk van aard zijn en in een VOG kunnen strafrechtelijke persoonsgegevens ontbreken. Wees echter wel bewust dat dergelijke documenten strafrechtelijke persoonsgegevens *kunnen* bevatten; de beoordeling van strafrechtelijke persoonsgegevens dient breder te worden gelezen dan strafbare feiten die direct een relatie hebben met handelingen die vallen onder het strafrecht.

Nationale identificatienummers
Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, mag uitsluitend worden gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.[49]
Het gebruik van deze nummers is dus enkel toegestaan wanneer dit in de wet is geregeld en dient zorgvuldig plaats te vinden. De gedachte hierachter is dat nationale identificatienummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijkt. Een verkeerde verwerking of misbruik van dit nummer kan grote gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene. Nationale identificatienummers die ter identificatie van een persoon bij wet zijn voorgeschreven zijn bijvoorbeeld[50]:
- Burgerservicenummer (BSN),[51]
- BIG-nummer (beroepen in de individuele gezondheidszorg),
- Vreemdelingennummer,
- Onderwijsnummer,
- Strafrechtketennummer.

[45] Artikel 10 AVG.
[46] Artikel 1 UAVG.
[47] Arrest van het Hof (Grote Kamer), C-439/19, 22-06-2021, ECLI:EU:C:2021:504.
[48] Idem.
[49] Artikel 46 UAVG.
[50] Het verdient hierbij opmerking dat deze lijst geen limitatieve opsomming is van nationale identificatienummers.
[51] Overheidsorganen kunnen bij het verwerken van persoonsgegevens gebruik maken van het BSN, met inachtneming van de Wet algemene bepalingen burgerservicenummer.

Bron persoonsgegevens
Met de bron van de persoonsgegevens wordt aangegeven waaruit en/of van welke personen of organisaties de persoonsgegevens worden verkregen.

Wanneer de persoonsgegevens niet direct van de betrokkene komen, dan is het van belang om de organisatie te noemen waar de gegevens vandaan komen, vanuit welke tool/platform de gegevens worden gedeeld, met welk doeleinde de persoonsgegevens oorspronkelijk zijn verzameld en op grond waarvan de persoonsgegevens verstrekt mogen worden.

Bijvoorbeeld:
- De persoonsgegevens worden verkregen via een interne database.
  De database is opgenomen in een Microsoft Excel-bestand. De database is in beheer van organisatie x. Organisatie x verwerkt deze persoonsgegevens met doeleinde y.

Het is van belang dat bekend is wat de herkomst is van de persoonsgegevens. 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 of wanneer dit is voorzien in Unie- of Nederlands recht.[52] 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 of in overeenstemming is met Unie- of lidstatelijk recht dat direct toeziet op desbetreffende verwerking van persoonsgegevens (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder).

Voorbeeld voor rapportagemodel

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoons-gegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatienummer)	Bron
Medewerker	Naam	Voornaam, achternaam, initialen	Gewoon	Direct van betrokkene via invulformulier
Medewerker	Contact-gegevens	E-mailadres	Gewoon	Direct van betrokkene via invulformulier
Medewerker	Demografische gegevens	Geboortedatum geslacht, nationaliteit	Gewoon	Via personeels-administratie
Medewerker	Financiële gegevens	Bankrekeningnummer	Gevoelig	Via salarisadministratie
Medewerker	Overige persoons-gegevens	RIN-nummer, IP-adres, MAC-adres	Gewoon	Direct van betrokkene via bezoek aan de website

3.3 Gegevensverwerkingen

Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

Om de rechtmatigheid van de gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben die plaatsvinden binnen de reikwijdte die in het voorstel (paragraaf 1) is opgenomen.

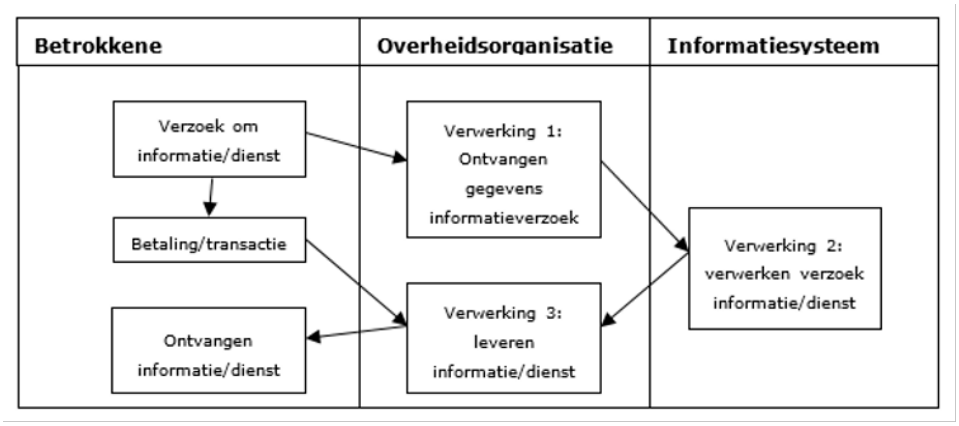
[52] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.

Onder verwerking van persoonsgegevens wordt verstaan: elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens.[53] Met een bewerking wordt iedere handeling bedoeld die met een persoonsgegeven kan worden verricht.

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.

Het is ten zeerste aan te raden om bij het beschrijven van de gegevensverwerkingen voor een abstractie-niveau te kiezen die zo dicht mogelijk bij de beschrijvingen van de gegevensverwerkingen passen, zoals die ook zijn opgenomen in het register van verwerkingsactiviteiten. Het is aan te raden om ook te verwijzen naar de verwerkingen zoals die zijn opgenomen in het register van verwerkingsactiviteiten, zodat het duidelijk is op welke verwerkingen de DPIA ziet.

Stroomschema
Omdat de gegevensverwerkingen binnen het voorstel gecompliceerd kunnen zijn en het niet altijd gemakkelijk is om het geheel van gegevensverwerkingen in woorden uit te drukken is het van belang om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een *input-proces-output* model, *stroomschema* of *workflow*. Zie hieronder voor een simpel voorbeeld.



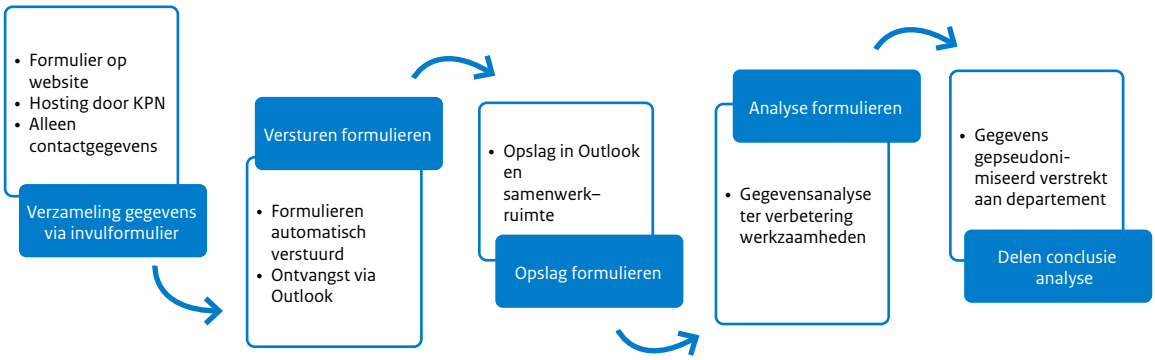
Een duidelijk stroomschema kan namelijk in een oogopslag laten zien hoe de gegevensverwerkingen binnen het proces lopen, waardoor gemakkelijk het overzicht kan worden bewaard in de DPIA. Verder kan ook gerefereerd worden naar het gebruikte stroomschema in de rest van de DPIA.

Om de duidelijkheid van het stroomschema te vergroten kan aan de volgende elementen worden gedacht:

- Benoem alle betrokken partijen (punt 6) in het stroomschema.
  Op die manier is het duidelijk welke partij verantwoordelijk of onderdeel is bij desbetreffende gegevensverwerking en wanneer de partijen precies worden betrokken bij de gegevensverwerkingen.
- Geef ook aan wat de AVG-rol is van iedere betrokken partij.
  Wanneer het stroomschema groter is dan de reikwijdte van de DPIA, geef duidelijk aan in het stroomschema over welke gegevensverwerkingen de DPIA gaat.
- Voeg per gegevensverwerking toe of specifieke applicaties, software, online platformen of cloud opslag wordt gebruikt.

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

Voorbeeld stroomschema opgenomen in rapportagemodel



Dit stroomschema is hierin opgenomen als voorbeeld ter illustratie hoe een simpel stroomschema van een proces met persoonsgegevens eruit kan zien. Gebruik dit voorbeeld alleen wanneer niet een eigen stroomschema wordt gemaakt.

Voorbeeld voor rapportagemodel

Gegevensverwerking	Persoonsgegevens
Verzoek om informatie	Naam, Contactgegevens, RIN-nummer, IP-adres, MAC-adres
Betaling/transactie	Naam, Contactgegevens, Demografische gegevens, Financiële gegevens, RIN-nummer, IP-adres, MAC-adres

3.4 Technieken en methoden van gegevensverwerking

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

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende risico'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.

Gegevensverwerkingen kunnen technisch complex zijn. Daarom kan het van grote toegevoegde waarde zijn om informatie in te winnen bij verschillende data-experts over de technieken en methoden van gegevensverwerking. Voorbeelden hiervan zijn:
- Een Chief Information Security Office (CISO);
- Information Security Officer (ISO);
- Data-analist;
- ICT-architect.

Geautomatiseerde besluitvorming
Uitsluitend geautomatiseerde besluitvorming is het nemen van besluiten met technologische middelen en zonder menselijke tussenkomst.[54] Indien uitsluitend geautomatiseerde besluitvorming voor

[54] Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van de Verordening (EU) 2016/679, p.9.

betrokkenen tot rechtsgevolgen leidt of hem anderszins in aanmerkelijke mate treft, dan is dat in beginsel verboden.[55]

Artikel 22 AVG voorziet in een algemeen verbod op uitsluitend geautomatiseerde individuele besluitvorming. Hiervan mag worden afgeweken indien sprake is van een van onderstaande uitzonderingen op het verbod, namelijk als het besluit:

a. Noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst;
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.[56]

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

d. Wettelijk is toegestaan, en voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.[57]

Indien bij de besluitvorming bijzondere categorieën van persoonsgegevens betrokken zijn, dan moet de verwerkingsverantwoordelijke aan aanvullende eisen voldoen.[58]

Kunstmatige intelligentie en algoritmen

Kunstmatige intelligentie, ook wel artificiële intelligentie genoemd, wordt gedefinieerd als software die is ontwikkeld aan de hand van een of meer technieken en benaderingen, die voor een bepaalde reeks door mensen gedefinieerde doelstellingen een resultaat kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen. Deze kunnen van invloed zijn op de omgeving waarmee interactie plaatsvindt tussen de software en de betrokkenen.[59] Algoritmen en kunstmatige intelligentie worden vaak door elkaar gebruikt, maar betekenen wel iets anders.
Algoritmen bestaan uit een reeks, meestal wiskundige, instructies. Wanneer deze instructies een bepaalde *input* krijgen, dan gaat deze door deze instructies heen en er volgt een *output* op basis van die instructies.
Kunstmatige intelligentie is niet gemakkelijk te definiëren, maar over het algemeen wordt deze term vereenzelvigd met *machine learning algorithms*.

Dit zijn algoritmen die (kunnen) leren aan de hand van het uitvoeren van de instructies. De software kan op verschillende manieren leren:

- Supervised learning: het algoritme leert aan de hand van gelabelde data met een specifiek uitgezochte dataset. Van tevoren is de data dus op zo'n manier gelabeld, dat de software op basis van die labels uitzoekt wat de correlaties zijn en hoe de data te herkennen en te gebruiken is.
- Unsupervised learning: het algoritme leert aan de hand van ongelabelde data. Zo kan de software zelf trachten structuur en correlaties te herkennen, zonder dat iemand de software de instructie heeft gegeven om specifieke labels te herkennen. Dit type algoritmen werkt met grotere datasets.
- Reinforcement learning: het algoritme leert van de eigen ervaring.
  Dat betekent dat wanneer het algoritme iets doet waarvoor het een 'beloning' krijgt, bijvoorbeeld dat wordt aangegeven dat iets goed is gedaan, dan probeert het algoritme dit gedrag vaker uit te voeren. Het doel van het algoritme is om zoveel mogelijk deze beloning te bemachtigen, waardoor het algoritme leert om de beloning op optimale manier te bereiken.

Bij de inzet van een systeem op basis van kunstmatige intelligentie of algoritmen is het van groot belang dat het systeemonderdeel uitmaakt van de DPIA en dat deze zorgvuldig wordt getest. Van groot belang is

[55] Artikel 22, eerste lid, AVG en artikel 11, eerste lid, Richtlijn.
[56] Artikel 22, tweede lid, AVG.
[57] Artikel 11, eerste lid, Richtlijn.
[58] Zie artikel 22, vierde lid, AVG.
[59] Artikel 3, eerste lid, Verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie.

het gebruik van trainingsdata voor de systemen die geen *bias* bevatten, zodat de besluitvorming die uit het systeem komt niet bevooroordeeld of discriminerend is.

Wanneer in de DPIA sprake is van enig gebruik van kunstmatige intelligentie en/of algoritmen, dan dienen deze na afronding van de DPIA toegevoegd te worden aan het algoritmeregister.

Daarnaast is het uitvoeren van een Impact Assessment Mensenrechten en Algoritmes (IAMA) aan te raden en in sommige gevallen zelfs verplicht. Deze assessment kan gelijktijdig met de DPIA worden uitgevoerd en kent op bepaalde punten een overlap. Zie voor meer informatie sectie 1.8.

Cloud
Onder een cloudoplossing wordt verstaan: het inzetten van een groot netwerk van servers die aan elkaar gekoppeld zijn om specifieke functies uit te voeren, zoals het opslaan en beheren van gegevens, het uitvoeren van toepassingen of het streamen van audiovisuele content. Een groot voordeel van cloud-oplossingen is dat deze schaalbaar zijn, mede deze cloudoplossingen plaatsvinden op een virtuele infrastructuur en met relatief gemak uitgebreid kan worden.

Hieronder volgen een aantal belangrijke aandachtspunten bij het inzetten van cloudoplossingen:
- **Dataclassificatie.** Gegevens worden gedeeld met een derde partij in een virtuele infrastructuur, waar mogelijk ook andere partijen indirect op zijn aangesloten. Het is daarom van belang dat helder is welke gegevens met welke dataclassificatie worden gedeeld via de cloudoplossing. Hier kan worden aangesloten op de BIO en de handreiking BIO-dataclassificatie.
- **Anonimisering.** Cloudaanbieders kunnen stellen dat persoonsgegevens bij het gebruik van hun dienst geanonimiseerd worden. Het is belangrijk om vast te stellen in welk stadium bij het gebruik van de cloudoplossing de persoonsgegevens geanonimiseerd worden.
- **Verantwoordelijkheid.** Let op de rol van de cloudaanbieder en de mate van verantwoordelijkheid bij het aanbieden van de dienst; hoe zwaarder de rol, des te meer regie de cloudaanbieder heeft.
- **Doelbinding.** Hoe meer gegevens bij de cloudaanbieder worden geplaatst, des te hoger het risico dat de cloudaanbieder onder eigen verantwoordelijkheid gegevensverwerkingen uitvoert die niet verenigbaar zijn met het oorspronkelijke doel. Zorg in de overeenkomst met de aanbieder dat dit duidelijk is afgebakend.
- **Afhankelijkheid.** Door het plaatsen van gegevens in de cloud ontstaat een technische afhankelijkheid, bijvoorbeeld om gegevens te verwijderen (uitvoeren bewaartermijnen) of bij de rechten van betrokkenen. Contractuele afspraken met de cloudaanbieder over deze elementen is essentieel om te kunnen voldoen aan wettelijke verplichtingen.
- **Aanvullende gegevensverwerkingen.** Cloudaanbieders hebben veel diensten en functionaliteiten om te leveren en het is aannemelijk dat deze worden aangeboden. Wanneer aanvullende functionaliteiten worden toegevoegd aan de dienstverlening door de cloudaanbieder, kunnen nieuwe gegevensverwerkingen ontstaan. Nieuwe gegevensverwerkingen moeten opnieuw worden beoordeeld in de DPIA en worden toegevoegd aan het register van verwerkingsactiviteiten.

De European Data Protection Board (EDPB) heeft in 2022 een gecoördineerde handhavingsactie opgezet voor het gebruik van op cloud gebaseerde diensten in de publieke sector. De bevindingen, die onder meer ingaan op het gebruik van telemetrie en logging, kan je hier lezen.

Indien gegevens opgeslagen of anderszins verwerkt worden in een publieke cloudvoorziening is daarop het cloudbeleid van toepassing.

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 de beroepsprestaties, economische situatie,

gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.[60]

Profilering is een procedure die een reeks statistische gevolgtrekkingen kan omvatten. Profilering wordt vaak toegepast om voorspellingen over mensen te doen door gebruik te maken van gegevens uit verschillende bronnen om een persoon eigenschappen toe te kennen op basis van de kenmerken van anderen die in statistisch opzicht vergelijkbaar zijn.[61]

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.

Denk bijvoorbeeld aan een overheidsorganisatie die persoonsgegevens gebruikt om risicoprofielen op te stellen van burgers om daar conclusies aan te verbinden.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.[62]

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.[63]
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. Het gaat niet alleen om nieuwe vormen van technologie die nog weinig in gebruik is, maar ook om bekende technologie die op een nieuwe manier wordt ingezet.

Om dit te bepalen kunnen de volgende vragen worden gesteld. Wanneer een van de antwoorden 'ja' is, dan is hoogstwaarschijnlijk sprake van de inzet van een nieuwe technologie.

a. Is de gebruikte technologie nieuw of nog niet eerder toegepast?
b. Is de gebruikte technologie bekend maar wordt deze op een nieuwe manier ingezet?
c. Zorgt de gebruikte technologie op zichzelf voor een verhoogd risico voor de privacy van betrokkenen?

[60] Artikel 4, vierde onderdeel, AVG en artikel 3, vierde onderdeel, Richtlijn.
[61] Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van de Verordening (EU) 2016/679, p.7.
[62] Artikel 11, derde lid, Richtlijn.
[63] 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).

Voorbeelden zijn:
- Intelligente volgsystemen op basis van GPS;
- Biometrie en nieuwe vormen van identificatie;
- Volgen van gezondheid van mensen via *wearables*;
- Automatisch rijdende voertuigen;
- Internet of things toepassingen.

3.5 Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.

De privacyregelgeving heeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld.[64] De vaststelling van de verwerkingsdoeleinden is een noodzakelijke voorwaarde om te kunnen beoordelen of de gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen getroffen dienen te worden om de risico's (onder C) te voorkomen of te verkleinen (onder D). Omschrijf daarom per gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Het is aan te raden om de voorbeeldtabel te gebruiken voor het beschrijven van de verwerkingsdoeleinden. Met de tabel kan per categorie persoonsgegevens worden aangegeven wat het verwerkingsdoeleinde is.

Wanneer de verzamelde persoonsgegevens oorspronkelijk zijn verzameld voor een ander doeleinde, dan is er de mogelijkheid om voor die specifieke persoonsgegevens aan te geven wat het oorspronkelijke doeleinde en het huidige (nieuwe) doeleinde is voor het verwerken van die persoonsgegevens en op grond waarvan de persoonsgegevens voor het nieuwe doeleinde mogen worden verwerkt.

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, zoals die zijn geïdentificeerd onder 3. Zo kan het algemene overkoepelende doel 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.

Bij conceptregelgeving wordt het doel van de gegevensverwerking zo mogelijk in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting.[65] Ook kan het doel zijn

[64] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.
[65] Artikel 6, derde lid, AVG en artikel 8, eerste lid, Richtlijn. Zie ook aanwijzing 162a Aanwijzingen voor de regelgeving.

vastgesteld in lagere regelgeving. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen de publieke taak worden gebleven die in de regelgeving is vastgesteld. Om de verwerkingsdoeleinden op een heldere wijze weer te geven is het aan te raden om de verwerkingsdoeleinden te koppelen aan de gegevensverwerkingen (punt 3).

Voorbeeld voor rapportagemodel

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
Verzoek om informatie	Voldoen aan verzoek van de betrokkene om informatie te geven	Niet van toepassing
Betaling/transactie	Voldoen aan verzoek van de betrokkene om tot betaling over te gaan en te waarborgen dat de betaling bij betrokkene aan komt	Niet van toepassing

3.6 Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, betrokkene(n) en ontvanger. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke persoonsgegevens.

Om de rechtmatigheid van de gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke partijen(functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker of ontvanger.[66] Wees er bewust van dat een organisatie of partij meerdere AVG-rollen tegelijk kan hebben, bijvoorbeeld dat de verwerkingsverantwoordelijke ook tegelijkertijd een verstrekker kan zijn. Een partij kan niet tegelijk verwerker en verwerkingsverantwoordelijke zijn voor dezelfde gegevensverwerking. Hieronder worden diverse rollen nader toegelicht. Als een rol van een partij onduidelijk is, is het raadzaam om contact op te nemen met een privacy officer of de FG, het vaststellen van de rol is belangrijk omdat dit doorwerkt in de verplichtingen van die partij onder de AVG.

Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die het doel van en de middelen voor de gegevensverwerkingen vaststelt.[67]

Elke verwerking van persoonsgegevens heeft minimaal een verwerkingsverantwoordelijke. Overige partijen die bij de verwerking zijn betrokken kunnen een verwerker, een sub-verwerker of een gezamenlijke verwerkingsverantwoordelijke zijn.

Om te beoordelen of een partij verwerkingsverantwoordelijke is, kan naar de volgende situaties gekeken worden:

A. Feitelijke invloed:
De verwerkingsverantwoordelijke bepaalt met welk doel de persoonsgegevens worden verwerkt en de manier waarop dat gebeurt. Als een andere partij voor dezelfde verwerking een verwerker is, moet deze

[66] De Autoriteit Persoonsgegevens heeft een tabel gepubliceerd met voorbeelden van situaties en uitleg welke organisatie in die situaties welke rol uitoefenen. (https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldlijst-wie-is-hier-de-verwerker-en-wie-de-verantwoordelijke)
[67] Artikel 4, zevende onderdeel, AVG en artikel 3, onderdeel 8, Richtlijn.

partij de instructies van de verwerkingsverantwoordelijke opvolgen. Deze instructies worden meestal gegeven in een verwerkersovereenkomst.

De gezagsverhouding kan blijken uit schriftelijke afspraken maar uiteindelijk is doorslaggevende wie in de praktijk daadwerkelijk de beslissingen neemt.

Hierbij moet opgemerkt worden dat een verwerker vaak zelf bepaalt welke middelen er worden gebruikt omdat een bepaalde dienst of een bepaald product zo in de markt is gezet. Bij de beoordeling moet in die situaties met name gekeken worden naar de feitelijke invloed op het doel van de verwerking.

B. Uitdrukkelijke juridische bevoegdheid
Als er in de wet staat dat een partij bepaalde persoonsgegevens mag of moet verwerken, dan is deze partij daarvoor de verwerkingsverantwoordelijke. Als een partij daarbij ondersteunt, zonder zelfstandig een beroep te kunnen doen op deze wettelijke bepaling, dan is deze partij een verwerker.

C. Impliciete bevoegdheid
Als er geen uitdrukkelijke juridische bevoegdheid bestaat om persoonsgegevens te verwerken dan kan een impliciete bevoegdheid een doorslaggevende factor spelen in het vaststellen of een partij als verwerkingsverantwoordelijke kwalificeert. Denk aan een werkgever die persoonsgegevens van zijn medewerkers verwerkt of een vereniging die de gegevens van haar leden verwerkt.

Verwerker
Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[68] Dat betekent dat de verwerker persoonsgegevens verwerkt direct onder instructies van de verwerkingsverantwoordelijke.

De verwerker is een persoon of organisatie buiten de organisatie van de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.[69] Deze afspraken moeten worden vastgelegd in een verwerkersovereenkomst. Daarnaast zijn er enkele standaard-afspraken over de wijze waarop een verwerker met persoonsgegevens dient om te gaan vastgelegd in de Algemene Rijksvoorwaarden voor het Verstrekken van Opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018).

Een partij is alleen verwerker voor zover het verwerken van persoonsgegevens de primaire opdracht van een andere organisatie is. En deze partij niet rechtstreeks onder het gezag van die organisatie valt.

De verwerker verwerkt persoonsgegevens in opdracht van de verwerkingsverantwoordelijke en niet voor eigen doeleinden. Indien de gegevens wel voor eigen doeleinden worden gebruikt dan is deze partij (voor dat gedeelte van de verwerking van persoonsgegevens) aan te merken als verwerkingsverantwoordelijke. Dit is vaak het geval als de diensten die de partij aanbiedt niet primair tot doel hebben om persoonsgegevens te verwerken.
Niet elke partij die door de Rijksoverheid wordt ingeschakeld is dus een verwerker.

Als een partij onder het rechtstreeks gezag van de verwerkingsverantwoordelijke valt dan is deze partij ook geen verwerker, dit is bijvoorbeeld het geval als iemand gedetacheerd is. De gedetacheerde persoon is in die situatie onderdeel van de verwerkingsverantwoordelijke.

Sub-verwerker
De sub-verwerker is de natuurlijke persoon, rechtspersoon of overheidsorgaan die ten behoeve van de verwerker specifieke taken uitvoert in het kader van de samenwerking tussen de verwerker en de verwerkingsverantwoordelijke.

[68] Artikel 4, achtste onderdeel, AVG en artikel 3, achtste onderdeel, Richtlijn.
[69] Artikel 28, derde lid, AVG en artikel 22, derde lid, Richtlijn.

Een sub-verwerker is dus de verwerker van de verwerker.

De verwerker dient schriftelijke toestemming te vragen aan de verwerkingsverantwoordelijke en schriftelijke afspraken met de sub-verwerker vast te leggen die wat betreft privacy verplichtingen ten minste hetzelfde strenge niveau hebben als de afspraken die zijn gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Hiervoor sluit de verwerker een verwerkersovereenkomst af met de sub-verwerker.

Gezamenlijke verwerkingsverantwoordelijken
Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, dan zijn zij gezamenlijke verwerkingsverantwoordelijken en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.[70]

Een belangrijk criterium voor de beoordeling of sprake is van gezamenlijke verwerkingsverantwoordelijkheid is het volgende: is het mogelijk voor het verwerkingsproces of processen die in deze DPIA worden beoordeeld om door te gaan zonder de samenwerking tussen de twee (of meer) organisaties? Wanneer organisaties namelijk individueel toch het proces kunnen uitvoeren, dan is sprake van individuele verwerkingsverantwoordelijkheid. Wanneer sprake is van onlosmakelijke processen, dan is waarschijnlijk sprake van gezamenlijke verwerkingsverantwoordelijkheid.[71]

Het is belangrijk dat gezamenlijke verwerkingsverantwoordelijken een regeling treffen waarin de verantwoordelijkheden voor de naleving van de AVG-regels worden vastgelegd. Hierin moet, bijvoorbeeld, worden vastgelegd wie verantwoordelijk is voor het afhandelen van een datalek en wie welke verantwoordelijkheden heeft bij het afhandelen van verzoeken van betrokkenen. De belangrijkste aspecten van de regeling moeten worden meegedeeld aan de betrokkenen, bijvoorbeeld door middel van een privacyverklaring.

Ontvanger
Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt.[72]

Verstrekker
Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens verstrekt aan een andere partij.

Derde
Een derde is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die geen betrokkene, verwerkingsverantwoordelijke, verwerker of een persoon is die rechtstreeks onder gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is om de persoonsgegevens te verwerken. De derde is wel een persoon of organisatie die betrokken is bij de gegevensverwerking, maar daar niet op een directe manier mee te maken heeft. De derde komt, bijvoorbeeld, naar voren bij de juridische grondslag ‘gerechtvaardigd belang van een derde’. Op basis van deze juridische grondslag kan een verwerkingsverantwoordelijke gegevens verwerken op basis van de belangen van een derde.

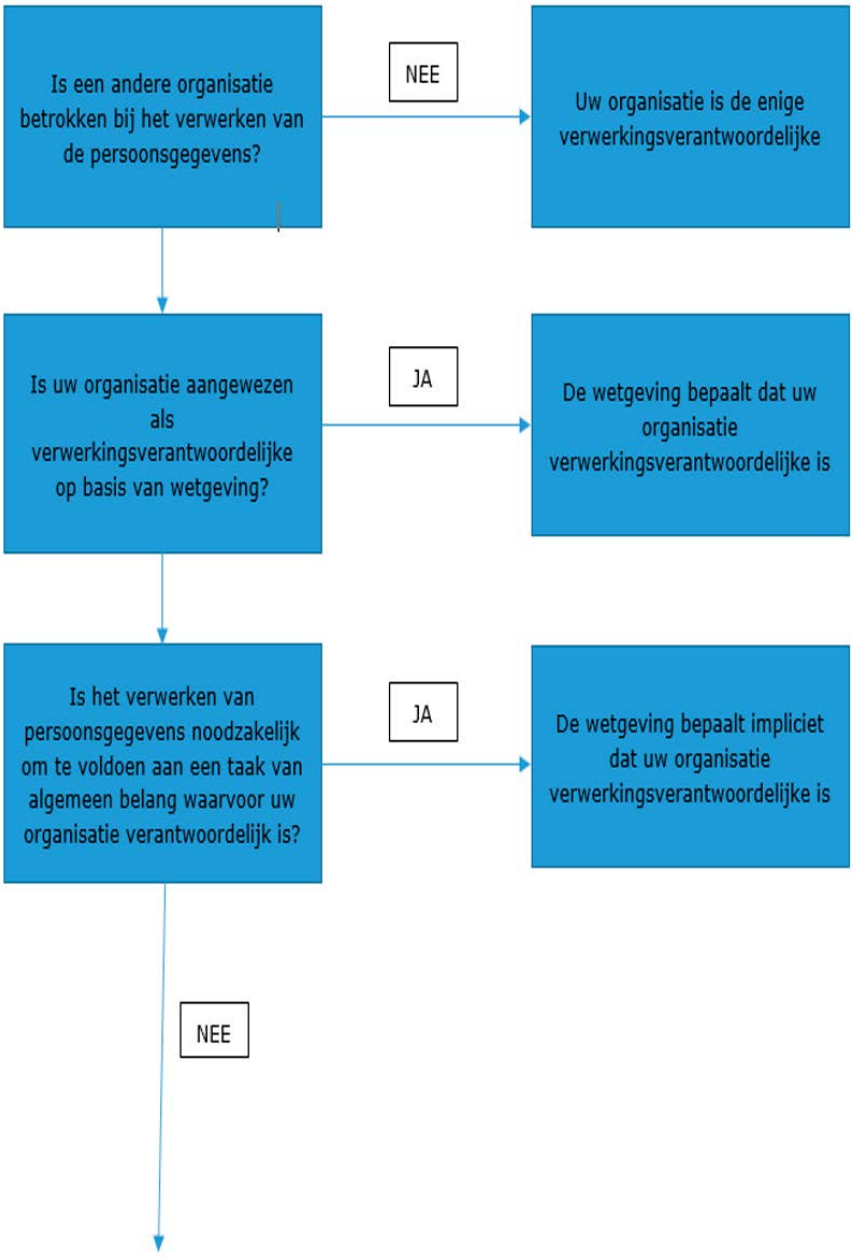
Bij conceptregelgeving kan het wenselijk zijn om daarin vast te leggen wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. Ook kan de rol van andere betrokken partijen worden vastgelegd, bijvoorbeeld dat zij gegevens kunnen of moeten verstrekken. Zo is in de Basisregistratie 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

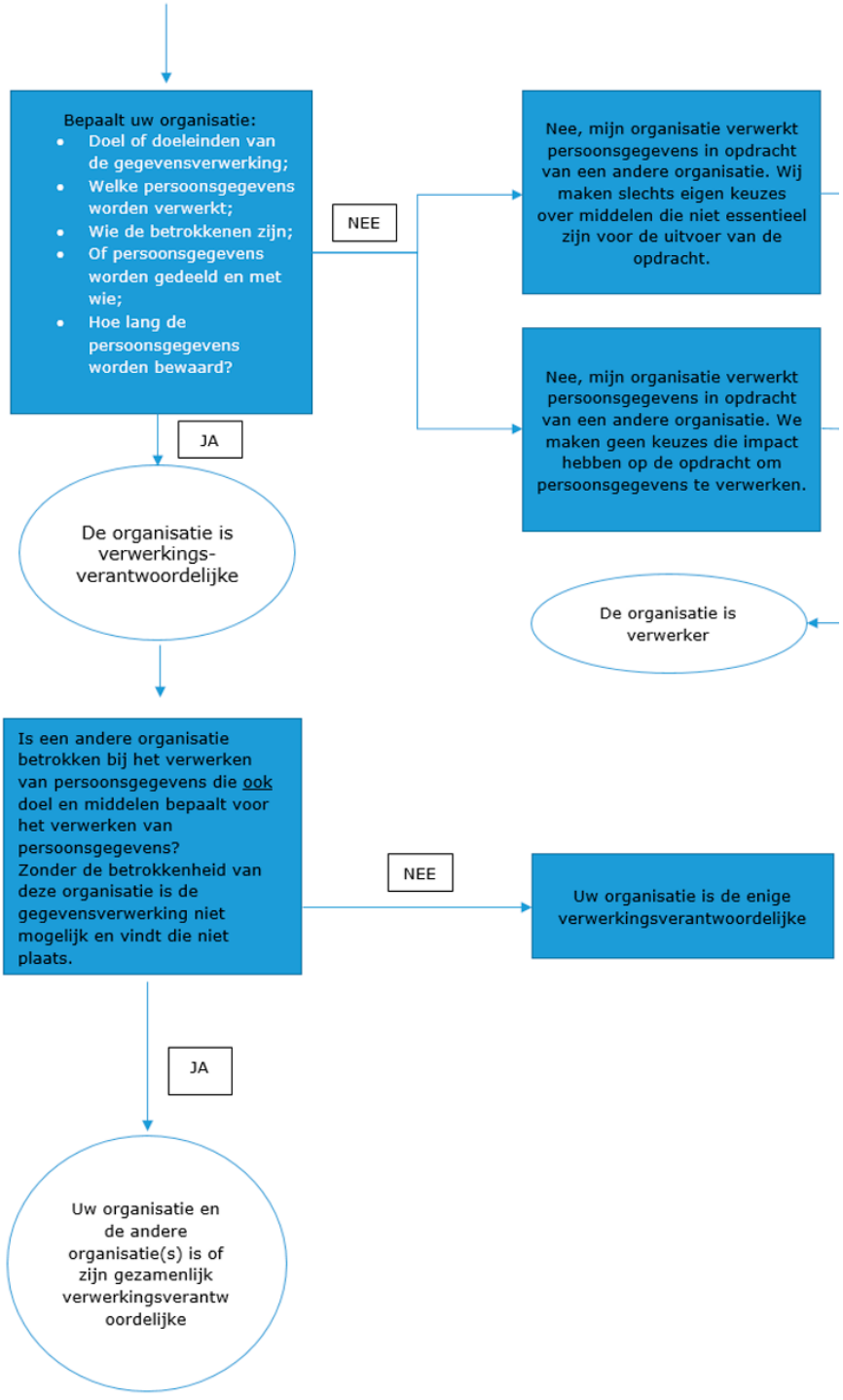
[70] Artikel 26, eerste lid, AVG en artikel 21, eerste lid, Richtlijn.
[71] Guidelines 07/2020 on the concepts of controller and processor in the GDPR (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf)
[72] Artikel 4, negende onderdeel, AVG en artikel 3, tiende lid, Richtlijn.

persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Voor zover niet al wettelijk voorgeschreven dienen de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg te moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Ook 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 ook worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Stroomschema om de AVG-rol te bepalen




Bepaalt uw organisatie:
Doel of doeleinden van de gegevensverwerking;
Welke persoonsgegevens worden verwerkt;
Wie de betrokkenen zijn;
Of persoonsgegevens worden gedeeld en met wie;
Hoe lang de persoonsgegevens worden bewaard?
NEE
Nee, mijn organisatie verwerkt persoonsgegevens in opdracht van een andere organisatie. Wij maken slechts eigen keuzes over middelen die niet essentieel zijn voor de uitvoer van de opdracht.
Nee, mijn organisatie verwerkt persoonsgegevens in opdracht van een andere organisatie. We maken geen keuzes die impact hebben op de opdracht om persoonsgegevens te verwerken.
JA
De organisatie is verwerkings-verantwoordelijke
De organisatie is verwerker
Is een andere organisatie betrokken bij het verwerken van persoonsgegevens die ook doel en middelen bepaalt voor het verwerken van persoonsgegevens? Zonder de betrokkenheid van deze organisatie is de gegevensverwerking niet mogelijk en vindt die niet plaats.
NEE
Uw organisatie is de enige verwerkingsverantwoordelijke
JA
Uw organisatie en de andere organisatie(s) is of zijn gezamenlijk verwerkingsverantwoordelijke

Voorbeeld voor rapportagemodel

Naam partij	Rol partij	Functies/afdelingen met toegang	Persoonsgegevens
Ministerie van Binnenlandse Zaken	Verwerkings-verantwoor-delijke	Bevoegde medewerkers die het project overzien	Naam, Contactgegevens, Demografische gegevens, Financiële gegevens, Overige gegevens
SSC-ICT	Verwerker	Bevoegde medewerkers die de technische infrastructuur voor het voorstel onderhouden	Naam, Contactgegevens, Demografische gegevens, Financiële gegevens, Overige gegevens
P-Direkt	Verwerker	Bevoegde medewerkers verzorgen de verzochte transacties	Naam, Contactgegevens, Financiële gegevens, Overige gegevens

N.B. Partijen die hier als voorbeeld worden genoemd als verwerkingsverantwoordelijke of verwerker kunnen in andere situaties, in de praktijk, een andere rol innemen. Iedere organisatie kan namelijk in bepaalde situaties een verwerkingsverantwoordelijke, verwerker, derde, verstrekker of andere AVG-rol innemen.

3.7 Belangen bij de gegevensverwerking

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen de belangen die met de gegevensverwerkingen gemoeid zijn een rol spelen. Kortom, wat zijn de voornaamste belangen en redenen dat het voorstel is geïnitieerd?

Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang.

Denk hierbij bijvoorbeeld aan:
- Bedrijfsbelangen,
- Financiële en commerciële belangen,
- Het handhaven van juridische vorderingen,
- Toezicht op medewerkers ten behoeve van de veiligheid
- Managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging,
- Gezondheidsredenen.

Vraag daarnaast betrokkenen of hun vertegenwoordigers naar hun mening over de verwerking.[73] Je kan betrokkenen rechtstreeks om hun mening vragen maar in sommige gevallen is het makkelijker om een of meerdere vertegenwoordigers te benaderen, zoals ouders als het om kinderen gaat, de (Groeps) Ondernemingsraad als het om medewerkers gaat of bijvoorbeeld een belangenafweging of stichting, die specifiek voor de belangen van de groep betrokkenen opkomt.

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

[73] Artikel 35 lid 9 AVG

3.8 Verwerkingslocaties

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn.

De fysieke locaties waar de gegevensverwerkingen plaatsvinden, kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Ook heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.[74]

Denk hierbij aan iedere locatie waar de desbetreffende verwerking van persoonsgegevens plaatsvindt; niet alleen de opslag van persoonsgegevens, maar bijvoorbeeld ook de locaties waar de gegevens worden geopend, gestreamd of tijdelijk worden opgeslagen.

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 Economische Ruimte[75] enkel onder bepaalde omstandigheden zijn toegestaan.[76]

Dit is het geval wanneer gebruik wordt gemaakt van een daarvoor bestemd doorgiftemechanisme. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit)[77] of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen.[78] Passende waarborgen zijn modelcontractbepalingen (SCCs) en gedragscodes. Verder kan ook gebruik worden gemaakt van bindende bedrijfsvoorschriften (BCR's).

Indien het doorgiftemechanisme niet gebaseerd is op een adequaatheidsbesluit dient er een Data Transfer Impact Assessment (DTIA) uitgevoerd te worden om vast te stellen of de nationale wetgeving in het land waarnaar de persoonsgegevens worden gestuurd geen afbreuk doen aan het gekozen doorgiftemechanisme. Zie voor meer informatie sectie 1.8.

Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene, noodzakelijk wegens gewichtige redenen van algemeen belang en noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.[79]

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 Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) over gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

[74] Artikelen 55 en 56 AVG en artikel 45 Richtlijn.
[75] De Europese Economische Ruimte bestaat uit alle landen die lid zijn van de Europese Unie plus de landen IJsland, Liechtenstein en Noorwegen.
[76] Artikel 44 AVG en artikel 35, eerste lid, Richtlijn.
[77] Artikel 45 AVG en artikel 36, Richtlijn.
[78] Artikel 46 AVG en artikel 37 Richtlijn.
[79] Artikel 49 AVG en artikel 38 Richtlijn.

Voorbeeld voor rapportagemodel

Gegevensverwerkingen	Verwerkingslocaties	Passende Waarborgen
Betalingen en transacties	Nederland	Niet van toepassing
Hosting van platform waar informatieverzoeken binnenkomen	Verenigd Koninkrijk	Adequaatheidsbesluit

3.9 Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn hoeven niet genoemd te worden.

Voor het benoemen van de wet- en regelgeving en beleid die van toepassing zijn op het verwerkingsproces is het aan te raden om deze in hiërarchische wijze in een overzicht op te nemen. Bijvoorbeeld:

- Internationale verdragen;
- Europese verdragen, verordeningen, richtlijnen en besluiten;
- Nationale wetgeving;
- AMvB's, gemeentelijke verordeningen, algemeen verbindende voorschriften; en
- Intern beleid.

Naast de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Hieronder is een lijst van voorbeelden van dergelijke wetten. Deze lijst is niet uitputtend.

- 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 grootstedelijke problematiek,
- Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet,
- Jeugdwet,
- Wet maatschappelijke ondersteuning 2015, en
- Participatiewet.

Er kan ook departementaal of Rijksbreed beleid zijn dat de mogelijkheden voor de 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 gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

Voorbeeld rapportagemodel

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Administratie declaraties medewerkers	Algemene wet inzake Rijksbelastingen	Art. 52
Verzamelen van persoonsgegevens via cookies op de website	Telecommunicatiewet	Art. 11.7a
Onderzoek naar veiligheid werkomstandigheden Rijksmedewerkers	Arbeidsomstandighedenwet	Art. 3

3.10 Bewaartermijnen

Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn.

Persoonsgegevens mogen niet langer worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is.[80] Met andere woorden: als het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd.

Op het beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering als 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.[81]

Niet alle persoonsgegevens in alle documenten bij alle gegevensverwerkingen moeten echter worden vernietigd of geanonimiseerd. Een gedeelte moet worden gearchiveerd op basis van de Archiefwet. Het is van belang om bewaartermijnen in de zin van de AVG op gescheiden wijze te benaderen ten opzichte van de Archiefwet. Een deel van de overheidsinformatie, bijvoorbeeld, gaat uiteindelijk naar het Nationaal Archief of naar een lokaal of regionaal archief. De reden hiervoor is dat deze informatie belangrijk is voor publieke verantwoording, rechtsvinding en vanuit cultuur-historisch oogpunt. De algemene regels hierover zijn opgenomen in de Archiefwet en sommige regels zijn verder uitgewerkt in het Archiefbesluit en de Archiefregeling.

Relatie bewaartermijn en archivering
De bewaartermijn in de zin van de AVG gaat specifiek over het bewaren van persoonsgegevens. Een document waarin geen persoonsgegevens zijn verwerkt of waar de persoonsgegevens geanonimiseerd zijn valt dus niet onder het bewaartermijnregime uit de AVG.

Wanneer documenten *wel* persoonsgegevens bevatten, dan dient wel een bewaartermijn te worden bepaald voor die persoonsgegevens. Die bewaartermijn is, onder meer, bepaald aan de hand van het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld en verwerkt.

Wanneer de bewaartermijn is afgelopen, dan betekent het dat de bewaartermijn op basis van het oorspronkelijke doeleinde is afgelopen. Als de Archiefwet of een andere archiveringsregeling van toepassing is en de gegevens gearchiveerd moeten worden, dan is archivering het nieuwe doeleinde waarvoor de persoonsgegevens worden verwerkt.

[80] Artikel 5, eerste lid, onder e, AVG en artikel 4, eerste lid, onder e, Richtlijn.
[81] Artikel 89 AVG en artikel 4, derde lid, Richtlijn.

Bijvoorbeeld, documenten over beleidskeuzes tijdens een bijzondere gebeurtenis of ramp kunnen persoonsgegevens bevatten van de besluitnemers en personen over wie de besluiten worden genomen. Deze documenten hebben vervolgens een bewaartermijn van, bijvoorbeeld, 20 jaar na het opstellen van de documenten. Na 20 jaar worden deze documenten naar het Nationaal Archief gebracht ter archivering.

Beschrijven bewaartermijn
De bewaartermijn die wordt vastgesteld refereert aan specifieke persoonsgegevens voor een specifieke gegevensverwerking. Bijvoorbeeld, het bewaren van een naam, adres en telefoonnummer in het kader van de sollicitatieprocedure heeft een bewaartermijn van maximaal vier weken na beëindiging van de sollicitatieprocedure. Het bewaren van een naam, adres en telefoonnummer in het kader van de arbeidsovereenkomst heeft een bewaartermijn van maximaal twee jaar na beëindiging arbeidsovereenkomst.

Verder moet worden vastgesteld wat na de bewaartermijn moet gebeuren.
Na de bewaartermijn kunnen twee handelingen plaatsvinden, namelijk de vernietiging/anonimisering of archivering van de persoonsgegevens om vervolgens de persoonsgegevens te vernietigen/te anonimiseren. Daarom is het ook belangrijk om te controleren of de Archiefwet, het Archiefbesluit en/of de Archiefregeling van toepassing is op de persoonsgegevens die worden verwerkt bij desbetreffende gegevensverwerking.

Stel de bewaartermijn vast door onder meer de volgende punten na te lopen:
- Ga na of een bestaande wettelijke of beleidsmatige bewaartermijn geldt voor desbetreffende gegevensverwerking.
- Wanneer het noodzakelijk is om persoonsgegevens te bewaren, bepaal concreet wat de duur is van de bewaartermijn, vanaf wanneer de bewaartermijn start, welke handelingen na de bewaartermijn moeten plaatsvinden en wie daarvoor verantwoordelijk is.
- Ga na of de gegevensverwerking is opgenomen in een selectielijst.
    - Hierin kan opgenomen zijn wat de bewaartermijn is voor een specifieke gegevensverwerking en wat na de bewaartermijn moet gebeuren.
- Wanneer de gegevensverwerking niet in een selectielijst is opgenomen en geen wettelijk vastgestelde bewaartermijn kent, ga na of het noodzakelijk is om de persoonsgegevens te bewaren en of het mogelijk is om de persoonsgegevens te anonimiseren of te verwijderen.
- Ga na of de Archiefwet, het Archiefbesluit of de Archiefregeling van toepassing is op de gegevensverwerking.

Bepaal de bewaartermijn zo concreet mogelijk. Hieronder enkele voorbeelden:
- Twee jaar na einde arbeidsovereenkomst worden de sollicitatiegegevens vernietigd;
- Vier weken na beëindiging sollicitatieprocedure worden de sollicitatiegegevens bij afgewezen kandidaten vernietigd;
- Een jaar na afronding evenement worden de persoonsgegevens vernietigd;
- Een jaar na laatste moment van inloggen worden de inloggegevens geanonimiseerd;
- Een jaar na publicatie onderzoeksrapport worden de ruwe onderzoeksgegevens gepseudonimiseerd en gearchiveerd voor een periode van 10 jaar. Na 10 jaar worden de onderzoeksgegevens geanonimiseerd en gepubliceerd via een open science platform.
- Twintig jaar na het verlenen van de bouwvergunning worden de persoonsgegevens en bijbehorende documenten naar de regionale archiefdienst gebracht voor archivering.

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 noodzakelijk moet zijn voor de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Voorbeeld voor rapportagemodel

Gegevens-verwerking	Verwerkings-doeleinde	Categorie Persoonsgegevens	Bewaartermijn	Motivatie bewaartermijn
Informatieverzoek vanuit betrokkene	Faciliteren van verzoek van betrokkene en het behouden van gegevens zodat contact opgenomen kan worden met betrokkene om informatie te verschaffen	Naam, E-mailadres	Gegevens worden aan het einde van de dag op de dag van het informatieverzoek automatisch verwijderd uit het systeem	Informatie over verzoeken van betrokkenen worden niet gebruikt na afhandeling verzoek. Geen noodzaak om langer te bewaren dan een dag na verzoek.
Verwerken declaratie-formulieren	Faciliteren van declaraties van medewerkers en waarborgen dat de formulieren correct worden verwerkt en gearchiveerd	Naam, Huisadres, TelefoonnummerE-mailadres, Declaratie-hoeveelheid, Bankrekeningnummer	Ten minste 7 jaar bewaard vanwege verplichting bewaren financiële administratie. Jaarlijks wordt gecontroleerd welk deel van de financiële administratie meer dan 7 jaar oud is en kan worden verwijderd.	Wettelijke verplichting op basis van de Algemene wet inzake Rijksbelastingen

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel en onderbouw aan de hand van de feiten zoals vastgesteld in onderdeel A of de gegevens-verwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel ook de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de DPIA is in het bijzonder juridische expertise nodig.

3.11 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.[82] Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is als deze gebaseerd kan worden op ten minste een van de volgende zes rechtsgronden:

1. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
2. 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.
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkings-verantwoordelijke rust.
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
5. 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.

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

6. 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.[83]

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

Binnen de DPIA worden verschillende gegevensverwerkingen beoordeeld. Per gegevensverwerking en per categorie persoonsgegevens kan een andere juridische grondslag of uitzonderingsgrond van toepassing zijn. Bijvoorbeeld, het verwerken van persoonsgegevens binnen de sollicitatieprocedure heeft normaliter als grondslag 'toestemming' of 'noodzakelijk voor de uitvoering van een overeenkomst'. Wanneer bij afronding van die sollicitatieprocedure een arbeidsovereenkomst wordt aangeboden, dan worden die persoonsgegevens verwerkt met 'wettelijke verplichting' als grondslag.

Hoewel overlap bestaat tussen de verwerkte persoonsgegevens worden deze verwerkt met een andere grondslag. Daarom raden we aan de verschillende gegevensverwerkingen van elkaar te onderscheiden, zodat duidelijk per gegevensverwerking kan worden aangegeven welke grondslag van toepassing is.

Wettelijke plicht en taak van algemeen belang
Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens Unie- of lidstatelijk recht, doorgaans is dat bij of krachtens de wet.[84]

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 expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens 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 ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn schrijft voor dat een gegevensverwerking alleen rechtmatig is als die verwerking gebaseerd is op de wet.[85] Controleer, bijvoorbeeld, de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet politiegegevens (Wpg) of desbetreffende gegevensverwerking hierin is opgenomen.

Gerechtvaardigde belangen
De rechtsgrond genoemd onder f, de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, is niet van toepassing op overheidsorganen en de gegevensverwerkingen die worden uitgevoerd in het kader van hun publieke taak. Overheidsorganen kunnen deze rechtsgrond alleen gebruiken voor gegevensverwerkingen in het kader van taken waarbij zij zich niet wezenlijk onderscheiden van private organisaties, zoals de beveiliging en bewaking van gebouwen.

Om deze rechtsgrond legitiem van toepassing te laten zijn is het verplicht dat de verwerkingsverantwoordelijke een belangenafweging maakt tussen de belangen en grondrechten van de betrokkene tegenover de belangen van de verwerkingsverantwoordelijke. Deze belangenafweging dient alleen gemaakt te worden over de gegevensverwerking waar deze rechtsgrond van toepassing is. Het is aan te raden de belangenafweging op te nemen in de DPIA, zodat deze gedocumenteerd is.

[83] Artikel 6, eerste lid, AVG.
[84] Artikel 6, derde lid, AVG.
[85] Artikel 8, eerste lid, Richtlijn.

Bij conceptregelgeving kan de regeling tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond wettelijke verplichting. Dit is het geval als de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht.

Bij overheidsverwerkingen zal het overheidsorgaan de gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. Zoals eerder aangegeven kan het gerechtvaardigd belang als grondslag niet worden gekozen bij gegevensverwerkingen in het kader van de uitoefening van de publieke taak.

In veel situaties zal de rechtsgrond toestemming ook niet kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen. Een belangrijke reden hiervoor is dat toestemming vrijelijk gegeven moet kunnen worden door de betrokkene. Wanneer de gegevensverwerking plaatsvindt tussen overheidsorganisatie en burger of tussen werkgever en werknemer, dan wordt over het algemeen aangenomen dat de burger/werknemer niet volledig vrij toestemming kan geven vanwege die hiërarchische verhouding.[86]

Voorbeeld voor rapportagemodel

Gegevensverwerking	Rechtsgrond	Relevante wet- en regelgeving (wettelijke verplichting/taak van algemeen belang)
Verzoeken tot informatie verwerken	Toestemming	Niet van toepassing
Betalingen en transacties	Noodzakelijk voor de uitvoering van de overeenkomst	Niet van toepassing
Hosting van platform waar informatieverzoeken binnenkomen	Toestemming	Niet van toepassing

3.12 Bijzondere persoonsgegevens

Als bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is of, in geval van nieuwe regelgeving, er zou moeten komen. Bij verwerking van een wettelijk identificatienummer, beoordeel of dit is toegestaan.

De AVG verbiedt de verwerking van bijzondere persoonsgegevens.

Op dit verwerkingsverbod gelden de volgende uitzonderingen in het kort:
- De betrokkene heeft uitdrukkelijke toestemming gegeven;
- De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en socialezekerheidsrecht, voor zover dit is toegestaan op basis van Unierecht of lidstatelijk recht;
- De verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- De verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- De verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- De verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht;
- De verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de

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

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, op grond van Unierecht of lidstatelijk recht;
- De verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid, op grond van Unierecht of lidstatelijk recht;
- De verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, op grond van Unierecht of lidstatelijk recht.[87]

Ga voor de volledige tekst van de uitzonderingen naar artikel 9 lid 2 AVG. Daarnaast zijn aanvullende uitzonderingen te vinden in de uitvoeringswet AVG (UAVG) en andere 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).[88]

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.[89]

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.[90]

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.[91]

Voorbeeld voor rapportagemodel

Gegevensverwerking	Type bijzonder persoonsgegeven	Uitzonderingsgrond
Verwerken vakbondslidmaatschap voor compensatie kosten lidmaatschap	Vakbondslidmaatschap	Uitdrukkelijke toestemming
Verwerken gezondheidsgegevens van zieke medewerkers bij verzuimregistratie	Gezondheidsgegevens	Noodzakelijk met het oog op de uitvoering van verplichtingen op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.

3.13 Doelbinding

Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of

[87] Artikel 9, tweede lid, AVG.
[88] Artikel 10 AVG.
[89] Artikel 10 Wet algemene bepalingen burgerservicenummer.
[90] Artikel 10 Richtlijn.
[91] Overweging 52 AVG en overweging 37 Richtlijn.

lidstaatrechtelijk recht, dan wel verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De privacyregelgeving heeft 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.[92]

De AVG regelt dat de verdere verwerking voor een ander niet-verenigbaar doel enkel toegestaan is als de verdere verwerking berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of lidstaatrechtelijke bepaling. Deze Unierechtelijke- of lidstatelijke bepaling moet een noodzakelijke en evenredige maatregel zijn 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.[93]

Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang[94], 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.[95]

Bij de toets of de verdere verwerking verenigbaar is, moet onder meer gekeken worden naar de volgende aspecten:
- Het verband tussen het oorspronkelijke doel en het nieuwe/toekomstige doel;
- De context waarin de persoonsgegevens worden verzameld (wat is de relatie tussen de verwerkingsverantwoordelijke en de betrokkene?)
- De soort en aard van de persoonsgegevens (gaat het om gevoelige of bijzondere persoonsgegevens?)
- De mogelijke gevolgen van de verdere verwerking (wat zijn de gevolgen voor de betrokkene?)
- Het bestaan van passende waarborgen voor de gegevensverwerking (bv. versleuteling van persoonsgegevens)

Bij overheidsverwerkingen moet de verwerkingsverantwoordelijke beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is. Dit gebeurt aan de hand van de bovengenoemde aspecten. Verder is het van belang dat na wordt gegaan of in sectorspecifieke wetgeving een geheimhoudingsplicht of een verbod op verdere verwerking is vastgelegd.

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).

[92] Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, Richtlijn.
[93] Artikel 6, vierde lid, AVG jo. artikel 23, eerste lid, AVG.
[94] Dit algemeen belang dient onderbouwd te worden conform de vereisten uit artikel 6 lid 1 sub e.
[95] Artikel 89 AVG.

Voorbeeld voor rapportagemodel

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
Statistisch onderzoek medewerkers	Demografische gegevens	Succesvol beantwoorden van onderzoeksvragen	Personeelsadministratie
Aanpassen en verbeteren website	IP-adres, MAC-adres	Aanpassen van de website op basis van informatie over apparatuur, locatie, browser, taal van websitebezoeker	Aanbieden van website aan websitebezoeker

3.14 Noodzaak en evenredigheid

Beoordeel of de gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op:

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 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 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.

Ter beoordeling van de proportionaliteit kunnen de volgende vragen worden gesteld:

- Staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Is de gegevensverwerking van persoonsgegevens te verwachten en voorzienbaar voor de betrokkenen?
- Hoe groot is het belang om de verwerkingsdoeleinden te bewerkstelligen?
- Is de gegevensverwerking het meest effectieve middel om het doeleinde te bereiken?

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?). Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Ter beoordeling van de subsidiariteit kunnen de volgende vragen worden gesteld:

1. Kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

i. Kunnen minder persoonsgegevens worden verwerkt en hetzelfde doeleinde worden bereikt?
ii. Zijn er wellicht manieren om minder gevoelige persoonsgegevens te verwerken?
iii. Kunnen de persoonsgegevens in het proces gepseudonimiseerd of geanonimiseerd worden?
iv. Kunnen de persoonsgegevens met minder partijen worden gedeeld of minder lang worden bewaard?

2. Zijn er alternatieve minder privacy invasieve verwerkingsprocessen onderzocht en gedocumenteerd?
   v. Welke alternatieven zijn overwogen en waarom zijn deze alternatieven niet gekozen?
   vi. Zijn alternatieven overwogen die hetzelfde doeleinde kunnen bereiken met minder persoonsgegevens?
   vii. Zijn alternatieven overwogen waarbij de gehele dienst binnen Nederland of de EU uitgevoerd kan worden?
   viii. Zijn alternatieven overwogen waarbij de verwerker geen gebruikmaakt van sub-verwerkers buiten de EU?

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

3.15 Rechten van de betrokkene

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

Een van de belangrijkste aspecten uit de AVG is dat betrokkenen een aantal rechten hebben als het gaat om de verwerking van hun persoonsgegevens. Met deze rechten kunnen betrokkenen namelijk controle houden over de verwerking van hun persoonsgegevens. Het is daarom van groot belang om bij de gegevensverwerkingen vast te stellen hoe gehoor gegeven wordt aan de privacyrechten.

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen.[96] Het betreft:

- Het recht op informatie,
- Het recht van inzage,
- Het recht op rectificatie en aanvulling,
- Het recht op gegevenswissing (vergetelheid),
- Het recht op beperking van de verwerking,
- Het recht op overdraagbaarheid van gegevens (dataportabiliteit),
- 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.[97] Uitzonderingen moeten altijd op een nationale wet berusten, of in de AVG direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving. Uitzonderingen op de rechten van betrokkenen zijn, onder meer, geregeld in artikel 41 UAVG.

Geef bij de beschrijving duidelijk aan wat de procedure is voor betrokkenen om hun rechten uit te oefenen wat betreft de gegevensverwerkingen. Ga hierbij in op hoe deze procedure binnen de desbetreffende organisatie is ingebed en welke rollen verantwoordelijk zijn binnen de verschillende stappen van de procedure.

[96] Hoofdstuk III (artikelen 12-22) AVG en hoofdstuk III (artikelen 12-18) Richtlijn.
[97] Artikel 23 AVG, artikel 13, derde lid, 15 en 16, vierde lid, Richtlijn.

Wanneer sprake is van gezamenlijke verwerkingsverantwoordelijkheid, dan moeten concrete afspraken worden gemaakt over welke partij de verantwoordelijkheid heeft voor het inrichten en voorzien van de uitoefening van de rechten van betrokkenen.

Als 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:

- De doeleinden van de verwerking of van de categorieën van verwerking;
- De categorieën van persoonsgegevens
- Het toepassingsgebied van de ingevoerde beperkingen
- De waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
- De specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken
- De opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
- De risico's voor de rechten en vrijheden van betrokkenen
- Het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking[98]

Recht op informatie en transparantie

Het recht op informatie hangt nauw samen met een van de belangrijkste AVG-beginselen uit artikel 5 van de AVG, namelijk dat persoonsgegevens op een transparante wijze verwerkt moeten worden. Het is een verplichting om de betrokkenen op een heldere en duidelijke manier te informeren over het verwerken van hun persoonsgegevens.

Wanneer persoonsgegevens direct bij de betrokkene wordt verzameld, dan is de verwerkingsverantwoordelijke verplicht om de volgende informatie te verstrekken aan de betrokkene:

- De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
- In voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming (FG) van de verwerkingsverantwoordelijke;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking;
- De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op deze rechtsgrond is gebaseerd;
- In voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- In voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Europese Commissie bestaat of een ander doorgiftemechanisme van toepassing is op de doorgifte;
- De bewaartermijn en de criteria voor de bepaling van deze termijn;
- Dat de betrokkene het recht om zijn/haar rechten uit te oefenen (i.e. de rechten die hierboven zijn genoemd);
- Wanneer de verwerking op (uitdrukkelijke) toestemming is gebaseerd, dat de betrokkene het recht heeft te allen tijde de toestemming in te trekken;
- Dat de betrokkene het recht heeft een klacht in te dienen bij de toezichthoudende autoriteit;
- Of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten; en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- Het bestaan van geautomatiseerde besluitvorming, inclusief de in artikel 22 AVG bedoelde profilering en nuttige informatie over de onderliggende logica en het belang en de verwachte gevolgen van de verwerking voor de betrokkene.

[98] Artikel 41, tweede lid, UAVG.

Wanneer persoonsgegevens niet direct bij de betrokkene wordt verzameld, dan is de verwerkingsverantwoordelijke ook verplicht om bepaalde informatie te verstrekken aan de betrokkene. Deze komen grotendeels overeen met bovenstaande informatie. Hieronder is de uitzondering opgenomen:

- De bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

Geef in de DPIA duidelijk aan hoe de betrokkenen geïnformeerd zullen worden over de gegevensverwerkingen. Bijvoorbeeld:

- Openbaar gepubliceerde privacyverklaring;
- Intern gepubliceerde privacyverklaring;
- Versturen van een fysieke brief naar huisadres betrokkenen;
- Versturen van een digitale brief naar e-mailadres betrokkenen;
- Betrokkenen worden gebeld.

Voorbeeld voor rapportagemodel

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Procedure vastgesteld: • Templates geschreven als voorbeeldreactie op verzoek van betrokkene • Verantwoordelijke medewerkers/afdeling aangewezen voor behandeling verzoeken • Procedure voor identificatie betrokkene vastgesteld • SaaS-oplossing (TopDesk) in gebruik genomen voor documentatie verzoeken van betrokkenen • Centraal contactpunt (website) gecreëerd voor verzoeken Betrokkenen worden geïnformeerd over de uitoefening van het recht van inzage via website x.	n.v.t.
Recht op rectificatie en aanvulling	Idem. Geen aanvulling op bovenstaande.	n.v.t.
Recht op vergetelheid	n.v.t.	Gegevens worden verwerkt om wettelijk vastgelegde taak uit te oefenen (zie wetgeving x)
Recht op beperking van de verwerking	• Procedure vastgesteld om vast te stellen of betrokkene recht heeft op beperking van de verwerking	n.v.t.
Recht op dataportabiliteit	Niet van toepassing, want verwerking is niet berust op toestemming of op een overeenkomst en de verwerking wordt niet via geautomatiseerde procedés verricht.	n.v.t.
Recht op beperking van de verwerking	Idem, zoals 'recht van inzage'. Geen aanvulling op bovenstaande.	n.v.t.
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	Binnen desbetreffende gegevensverwerking worden alle besluiten direct of indirect middels een menselijke blik genomen.	n.v.t.
Recht om bezwaar te maken	Niet van toepassing, want gegevensverwerkingen hebben 'noodzakelijk om te voldoen aan een wettelijke verplichting' als grondslag	n.v.t.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht op duidelijke informatie	Betrokkenen worden middels een privacyverklaring op website x geïnformeerd over de gegevensverwerkingen.	n.v.t.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de 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.

3.16 Risico's voor betrokkenen

Beschrijf en beoordeel alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen, zoals het recht op privacy en het verbod op discriminatie. Ga in ieder geval in op:

- *Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;*
- *De oorsprong van deze gevolgen;*
- *De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden; en*
- *De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.*

Volgens de privacyregelgeving dient een DPIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten.[99] Bij het identificeren van risico's gaat het niet om de risico's voor de organisatie(s) en partij(en) die verantwoordelijk zijn voor de gegevensverwerkingen, maar om de risico's voor de rechten en vrijheden van betrokkenen.

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.[100] Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.[101]

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.[102] Daarom zal ook gebruik gemaakt kunnen 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 etc.), ziet de risicoafweging van de DPIA op de risico's voor de betrokkenen.

Risico's identificeren

De eerste stap is om potentiële risico's vast te stellen. Een risico is de situatie waarin persoonsgegevens worden verwerkt die direct of indirect (kunnen) leiden tot schadelijke gevolgen voor de rechten en

[99] Artikel 35, zevende lid, aanhef en onder c, AVG en artikel 27, tweede lid, Richtlijn.
[100] Overweging 76 AVG.
[101] Overweging 84 AVG.
[102] Artikel 4, aanhef en onder a, van het Besluit voorschrift informatiebeveiliging rijksdienst 2007.

vrijheden van de betrokkenen. Deze risico's zijn gebaseerd op de situatie zoals die op het moment van het schrijven van de DPIA geldt, inclusief de bestaande maatregelen die op dat moment van toepassing zijn op desbetreffende risico's. Bij de volgende stap (17) worden de maatregelen geïdentificeerd die aanvullend genomen worden om de geïdentificeerde risico's te mitigeren.

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 relationale 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;
- 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.[103]

Bij (onrechtmatige) verwerkingen van persoonsgegevens kan gedacht worden aan het al dan niet opzettelijke:

- Vernietiging en verlies (beschikbaarheid);
- Wijziging (integriteit);
- Ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, of anderszins handelen in strijd met het recht.[104]

Discriminatie

Indien sprake is van discriminatie, dan wordt er in strijd met het recht gehandeld. Discriminatie is het ongerechtvaardigd onderscheid maken tussen gelijke gevallen, dat is verboden op grond van artikel 1 van de Nederlandse Grondwet. Het recht gaat niet alleen uit van een beperkt aantal gronden waarop in principe geen besluiten mogen worden genomen (zoals godsdienst, levensovertuiging, ras of geslacht) maar verbiedt ook discriminatie 'op welke grond ook'. Niet alleen directe discriminatie is verboden, maar ook indirecte discriminatie Dat betekent overigens niet dat het maken van onderscheid altijd verboden is. Zo is wel wettelijk toegestaan om onderscheid te maken op basis van leeftijd bij arbeid (denk aan het beëindigen van de arbeidsverhouding bij het bereiken van de AOW-gerechtigde leeftijd).

Directe discriminatie

Van directe discriminatie is sprake als een persoon op een andere wijze wordt behandeld dan een ander in een vergelijkbare situatie.

[103] Overwegingen 75 en 85 AVG en overweging 51 Richtlijn.
[104] Overweging 83 AVG en overweging 60 Richtlijn.

Indirecte discriminatie
Van indirecte discriminatie is sprake als een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze een groep personen in vergelijking met andere groepen personen bijzonder treft. Een voorbeeld daarvan is een beveiligingssysteem op basis van gezichtsherkenning waarbij strenge kledingvoorschriften worden gesteld met als doel het hoofd en gezicht vrij te houden zodat het systeem het gezicht goed kan analyseren. Personen met hoofd- of gezichtsbedekking vanwege religieuze redenen worden door zulke voorschriften in het bijzonder getroffen.

Verder oordeelde de rechter in de uitspraak over het Systeem Risico Indicatie (SyRI, een wettelijk instrument dat de overheid gebruikte voor de bestrijding van fraude op bijvoorbeeld het terrein van uitkeringen, toeslagen en belastingfraude) dat gegeven de grote hoeveelheden gegevens die in aanmerking kwamen voor verwerking in SyRI, waaronder ook bijzondere persoonsgegevens, en de omstandigheid dat gebruik werd gemaakt van risicoprofielen, het risico bestond dat met de inzet van SyRI onbedoeld verbanden werden gelegd op basis van *bias*, zoals een lagere sociaal economische status of een immigratieachtergrond. De rechter vond daarbij van belang dat op basis van de SyRI-wetgeving niet kon worden beoordeeld of dit risico voldoende was ondervangen, bij gebrek aan controleerbaar inzicht in de risico-indicatoren en de (werking van) het risicomodel. Aanvullend op de uitspraak over SyRI is in het verslag Parlementaire Ondervraging Kinderopvangtoeslag naar voren gekomen dat het gebruik van nationaliteit als risico-indicator voor risicoprofielen ervoor zorgt dat dit een onbehoorlijke en discriminerende verwerking is.[105]

Als er mogelijk sprake is van directe of indirecte discriminatie als gevolg van de verwerking van persoonsgegevens waar de DPIA op ziet, dan is het noodzakelijk om een anti-discriminatietoets uit te voeren, waarin uiteen wordt gezet 1) of er sprake is van onderscheid en op basis waarvan 2) waarom (voor welk doel) er onderscheid gemaakt wordt of gaat worden 3) of er sprake is van direct of indirect onderscheid 4) of deze vorm van onderscheid bij wet is toegestaan 5) welke maatregelen er genomen worden om discriminatie te voorkomen of de gevolgen daarvan te mitigeren. Zie voor meer informatie https://www.mensenrechten.nl/mensenrechten-voor-jou/discriminatie-en-gelijke-behandeling

Big Data
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.

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 en de aard van de persoonsgegevens. Persoonsgegevens die bijvoorbeeld de sleutel vormen voor toegang tot geldelijke middelen of waarmee de betrokkene reputatieschade kan oplopen, brengen risico's met zich mee. Denk hierbij aan de inloggegevens voor DigiD of informatie over de psychologische situatie van betrokkene.

[105] Kamerstukken II, 35 510, nr. 2, Parlementaire ondervragingscommissie Kinderopvangtoeslag, 'Ongekend Onrecht. Verslag - Parlementaire ondervragingscommissie Kinderopvangtoeslag', 17-12-2020, p.14.

We raden aan om de inschatting als volgt in te delen. Het inschatten van de ernst van het risico kan worden gedaan aan de hand van de kans en de impact dat het risico heeft. Geef zowel de kans dat het risico plaatsvindt als de impact dat het risico heeft een classificatie: laag, gemiddeld of hoog. Vervolgens is de classificatie voor het risico op zichzelf gebaseerd op de formule kans x impact. Door deze berekening te doen aan de hand van de tabel in het rapportagemodel wordt de totale ernst van het risico ingeschat.

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

Risico's beoordelen
Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn. Zie het voorbeeld hieronder. Het is belangrijk om een motivatie toe te voegen voor de risico-inschatting, zodat gedocumenteerd is op basis van welke afwegingen de risico-inschatting tot stand is gekomen.

Voorbeeld voor rapportagemodel

Beschrijving risico	Kans	Impact	Risico-inschatting
Verzamelde gegevens worden niet na eindigen bewaartermijn niet verwijderd	Gemiddeld	Gemiddeld	Gemiddeld
Ongeautoriseerde gebruiker krijgt toegang tot het systeem waarin persoonsgegevens zijn opgeslagen	Laag	Gemiddeld	Laag
Financiële persoonsgegevens worden voor ander doeleinde gebruikt dan bepaald (function/mission creep)	Gemiddeld	Hoog	Hoog

D. Maatregelen en restrisico's

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 DPIA is in het bijzonder expertise over informatiebeveiliging belangrijk.

3.17 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.

De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.[106]

In dit punt worden verschillende maatregelen beschreven:
- De maatregelen die al worden genomen door de betrokken partijen die direct betrekking hebben op de risico's van de gegevensverwerkingen. Bijvoorbeeld, beveiligingsbeleid dat direct van toepassing is op de gegevensverwerkingen.
- De maatregelen die zullen worden genomen om de risico's van de gegevensverwerkingen zoveel mogelijk te mitigeren.

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

Passende technische en organisatorische maatregelen
De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.[107] 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 de risico's. Naarmate deze 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.[108]

Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Risico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een resterend risico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe het tot dit restrisico is gekomen en waarom deze aanvaardbaar wordt geacht. Deze worden onder punt 17 geïdentificeerd.

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 certificeringsmechanismes. Wanneer een of meerdere maatregelen van toepassing zijn op de gegevensverwerkingen, beschrijf dan specifiek welke beveiligingsstandaarden, praktijken, gedragscodes en/of certificeringsmechanismes van toepassing zijn en op welke manier deze in de praktijk van toepassing zijn op de gegevensverwerkingen.

Ter illustratie noemt de AVG de volgende maatregelen:
- Pseudonimiseren en versleutelen van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- 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.[109]

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[110]:
- 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;

[107] Artikel 32 AVG en artikel 29 Richtlijn.
[108] Overwegingen 83 en 94 AVG.
[109] Artikel 32, eerste lid, AVG.
[110] Artikel 5, eerste lid, onder d, AVG en artikel 4, eerste lid, onder d, Richtlijn.

- Resonsible-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 Overheid (BIO). De maatregelen hoeven zich overigens niet te beperken tot beveiligingsmaatregelen. Denk 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.

De Richtlijn noemt tot slot de volgende maatregelen:
- Controle op de toegang tot de apparatuur;
- Controle op de gegevensdragers;
- Opslagcontrole;
- Gebruikscontrole
- Controle op de toegang tot gegevens;
- Transmissiecontrole;
- Invoercontrole;
- Transportcontrole; en
- Herstelmogelijkheid.[111]

In de Richtlijn is opgenomen dat lidstaten logbestanden van bepaalde vormen van verwerkingen dienen bij te houden, zodat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen. Indien mogelijk ook de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekend heeft gemaakt, en de identiteit van de ontvangers van die persoonsgegevens.[112]

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.

Het is belangrijk dat een departementale Chief Information Security Officer (CISO) de genoemde technische en maatregelen toets voordat de DPIA definitief wordt vastgesteld.

Big Data
Bij *Big data*-analyses (zie punt 4) 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. Documenteer hoe deze foutmarge tot stand is gekomen.
- 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.[113]

[111] Artikel 29, tweede lid, Richtlijn.
[112] Artikel 25, eerste lid, Richtlijn.
[113] *Kamerstukken II* 2016/17, 26 643, nr. 426, p. 7-10.

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.[114]
- 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.

Resterende risico's

Na het identificeren van risico's (punt 16) en de maatregelen (punt 17) om deze risico's te mitigeren, dient te worden beoordeeld welke resterende risico's aanwezig zijn. Het is namelijk niet mogelijk om risico's met volledige zekerheid te mitigeren en dat is acceptabel. Organisaties hebben namelijk niet oneindig hoeveelheid tijd, energie en mogelijkheden om risico's volledig te mitigeren.

Bij het beoordelen van de resterende risico's is het te adviseren om aan de volgende punten aandacht te besteden:

- Geef aan welke risico's (paragraaf 16) niet volledig door de genomen maatregelen (paragraaf 17) voorkomen worden.
- Vermeld specifiek in welke situatie met welke persoonsgegevens een resterend risico aanwezig is.
- Schat het resterende risico in met de formule kans x impact en door de niveaus laag, gemiddeld en hoog te gebruiken.
- Beschrijf helder en duidelijk waarom deze resterende risico's na het nemen van de maatregelen acceptabel zijn.

Wanneer bij de beoordeling van de restrisico's naar voren komt dat de restrisico's een hoog risico opleveren, ondanks de genomen maatregelen, dan moet de Autoriteit Persoonsgegevens geraadpleegd worden over de gegevensverwerkingen die overwogen worden te initiëren. Dit heet voorafgaande raadpleging.

Naar aanleiding van de restrisico's en de beschreven aanvullende maatregelen ter verdere mitigatie van deze restrisico's is het aan te raden om een plan van actie op te stellen. Op basis van dit plan kunnen de aanvullende maatregelen door daarvoor aangewezen verantwoordelijken worden geïmplementeerd, zodat de restrisico's op een zo laag mogelijk niveau komen. Neem in het plan van actie per geformuleerde aanvullende maatregel op welke partij verantwoording draagt voor het uitvoeren van deze maatregel.

Voorbeeld voor rapportagemodel

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Verzamelde gegevens worden niet na einde bewaartermijn verwijderd	Procedure geïmplementeerd en verantwoordelijke functionarissen aangewezen, zodat periodiek wordt gecontroleerd of bewaartermijn wordt gehonoreerd	Verantwoordelijke functionaris heeft geen toegang tot alle bronlocaties van alle gegevens om gegevens te verwijderen, waaronder automatische back-ups	Organisatie x / Rol y
Ongeautoriseerde gebruiker krijgt toegang tot systeem met verzamelde persoonsgegevens	Verzamelde persoonsgegevens in systeem zijn gepseudonimiseerd en sleutelgegevens zijn buiten het systeem opgeslagen Twee factor authenticatie geïmplementeerd voor inloggen in systeem	Gebrek aan BYOD beleid, zorgt ervoor dat het beveiligingssysteem niet weet wanneer een geautoriseerd apparaat of ongeautoriseerd apparaat toegang heeft	Organisatie x / Rol y

[114] Artikel 22 AVG.

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Financiële gegevens worden voor andere doeleinden gebruikt dan vooraf bepaald (function creep/mission creep)	Systeem met financiële gegevens wordt gemonitord logging waardoor handelingen met persoonsgegevens te zien en terug te herleiden zijn naar een persoon	Gebrek aan beleid en trainingen op het gebied van function en mission creep leidt ertoe dat verantwoordelijke functionarissen onvoldoende bekend zijn met doelbinding en verenigbare gegevensverwerkingen	Organisatie x / Rol y

De tabel dient als volgt te worden ingevuld.

Onder 'risico' wordt een beschrijving gegeven van een bestaand risico binnen de gegevensverwerkingen.

Onder 'maatregelen' dienen alle maatregelen te worden genoemd die geïmplementeerd worden om het risico zoveel mogelijk te verminderen.

De 'beheerder van maatregelen' is de persoon of het organisatieonderdeel die verantwoordelijk (niet verwerkingsverantwoordelijke) is voor het feit dat de maatregelen worden uitgevoerd.

Onder 'resterend risico en risico-inschatting' dient te worden beschreven welke resterende risico's overblijven na het nemen van de maatregelen. De kleur van het vlak geeft aan wat de risico-inschatting is voor het resterende risico. Deze risico-inschatting wordt weer uitgevoerd op basis van het principe kans x impact. Beschrijf het resterende risico in het vlak en geef met de kleuren groen (laag risico), geel (gemiddeld risico) en rood (hoog risico) aan wat de risico-inschatting is op basis van het principe kans x impact. Dit wordt niet uitdrukkelijk opgenomen in de tabel om de tabel overzichtelijk te houden.

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011 | 2500 ea Den Haag

Mei 2023