

Bovendien voorkomt het uitvoeren van een DPIA in een vroegtijdig stadium dat latere kostbare aanpassingen worden gedaan in processen, herontwerp van systemen of zelfs het stopzetten van een project. Nog belangrijker is dat het uitvoeren van een DPIA in de ontwerpfase betekent dat het IMG per definitie rekening houdt met gegevensbescherming. Dit is namelijk ingebed in de structuur van een project. Hiermee wordt voldaan aan de vereiste van *privacy by design*.

2. Achtergrond van de DPIA

2.1 Motivering voor een DPIA

Een DPIA kan ondersteuning bieden om de bescherming van persoonsgegevens op een gestructureerde manier onderdeel te laten zijn van de inrichting van een nieuw proces of project waar persoonsgegevens verwerkt worden binnen het IMG. Door de DPIA deel uit te laten maken van de belangenafweging en de besluitvorming bij voorgenomen beleid, wordt de kwaliteit van de besluitvorming verhoogd.

Een DPIA kan richtinggevend en corrigerend zijn. Een DPIA kan richtinggevend zijn als het hanteren van een DPIA model relevante privacy risico's aan het licht brengt die niet in een eerder stadium zijn ontdekt. Indien dat het geval is, kunnen deze aspecten alsnog in de voorbereiding meegenomen worden. Een DPIA helpt op deze manier met het signaleren en beheersen van risico's en het vermijden van onnodige kosten die gepaard kunnen gaan met het oplossen van problemen die in een later stadium worden ontdekt.

Ook kan tijdens de uitvoering van een DPIA blijken dat het nodig is om eerdere keuzes te heroverwegen om vervolgens voor minder inbreuk makende oplossing te kiezen om een bepaalde doelstelling te bereiken. Dit is de zogenaamde corrigerende DPIA. Vanwege het karakter van een DPIA kan het uitvoeren ervan een proces zijn waarbij beoogde (beleids-)oplossingen of ontwerpen van een systeem geleidelijk worden aangescherpt met als doel de privacy risico's voor de betrokkenen te verminderen.

Het uitvoeren van een DPIA kan zorgen voor vertrouwen in de voorgenomen maatregel, binnen en buiten het IMG. Het verzamelen van de informatie voor het beantwoorden van de vragen helpt medewerkers en leidinggevendenden bij de besluitvorming en het afleggen van verantwoording daarover. Bovendien stimuleert het uitvoeren van een DPIA het privacy bewustzijn binnen het IMG.

Het uitvoeren van een DPIA maakt aantoonbaar welke risico's het IMG aantreft en welke risicobeperkende maatregelen worden genomen om de risico's te beperken. Deze accountability sluit aan bij het privacy beleid van het IMG en sluit aan bij de voorwaarden die hierover in de AVG zijn opgenomen.

Tenslotte stelt de AVG als gevolg aan het niet voldoen aan de eisen van een DPIA of het niet (correct) uitvoeren van een DPIA als dat wel verplicht is, dat de AP een administratieve boete kan opleggen van maximaal 10 miljoen EUR.

2.2 Verplichting om een DPIA uit te voeren

2.2.1 Inleiding

Een DPIA moet verplicht worden uitgevoerd:

1. bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien;
2. bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

In de tweede situatie is een DPIA dus niet in alle gevallen verplicht, maar alleen als er een verwerking met een hoog risico is. Daarvoor is de AVG leidend.

De AVG noemt een aantal gevallen waarin een DPIA altijd verplicht is:

- Bij de evaluatie of scoretoekenning van persoonlijke aspecten gebaseerd op geautomatiseerde verwerking, waaronder profilering en op basis daarvan besluiten gebaseerd worden;
- Het op grote schaal verwerken van bijzondere of strafrechtelijke persoonsgegevens;
- Bij het gebruik maken van kunstmatige intelligentie of risicomodellen;
- Het op grote schaal en systematisch volgen van mensen in publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht.

Een DPIA is dus verplicht als de verwerking van persoonsgegevens een waarschijnlijk hoog risico inhoudt voor de privacy van betrokkenen. De AP heeft [een lijst gepubliceerd](#) ter ondersteuning van de beoordeling of sprake is van een hoog risico. Deze lijst is niet uitputtend, dat betekent dat er gegevensverwerkingen waarvoor een DPIA wel verplicht is niet op de lijst staan. In dat geval moet

het IMG beoordelen of de gegevensverwerking een hoog risico meebrengt voor de betrokkenen. Dat kan aan de hand van de criteria van de werkgroep van Europese toezichthouders. Die heeft [een lijst met 9 criteria](#) vastgesteld om te toetsen of een DPIA moet worden uitgevoerd. In het geval de verwerking aan twee of meer criteria voldoet, kan als vuistregel worden gezien dat dan een DPIA verplicht is. Toch zijn dit enkel handreikingen om een inschatting te maken en kan het dus zijn dat als maar aan één criterium is voldaan, een DPIA toch nog verplicht kan zijn.

2.2.2 Bestaande gegevensverwerkingen

Op het moment dat de gegevensverwerking al voor 25 mei 2018 is begonnen, moet het IMG [onder voorwaarden](#) ook een DPIA uitvoeren. Dat zal bijna altijd het geval zijn omdat de risico's van de verwerking zijn veranderd omdat de maatschappelijke context is veranderd, de verwerking totaal veranderd is en/of een DPIA volgens de AP iedere drie jaar geëvalueerd dient te worden. Daarom zal voor een verwerking die al voor 2018 is gestart met een verhoogd risico, altijd een DPIA uitgevoerd dienen te worden. Voor de meeste situaties zal het gaan om verwerkingen die pas na 25 mei 2018 zijn begonnen. In dat geval worden de normale regels zoals beschreven onder 2.2.1. gevolgd.

2.2.3 Nieuwe gegevensverwerkingen

Bij nieuwe verwerkingen moet beoordeeld worden of een DPIA uitgevoerd moet worden voorafgaand aan de aanvang van de gegevensverwerking. Bovendien zou tijdens de ontwikkeling van het project of het proces de DPIA meermaals uitgevoerd moeten worden (zie ook hierboven onder 1.4).

Bij de ontwikkeling van een nieuw project wordt allereerst een **Project Start Architectuur (PSA)** uitgewerkt, waar de onderdelen Privacy en Informatiebeveiliging (Security) in zijn meegenomen. Bij de PSA wordt gevraagd om een preDPIA (Quickscan) in te vullen om een inschatting te maken van de risico van de verwerking en of een DPIA verplicht is. Het risico van de verwerking kan worden bepaald aan de hand van het bijbehorende vragenlijst (bijlage 3). Door de vragen te beantwoorden, is het mogelijk om te bepalen of een verwerking wel of geen hoog risico is. Ook volgt uit de risicoanalyse waar het IMG maatregelen moet nemen. Deze preDPIA wordt door het privacy team (Privacy Officer) beoordeeld.

2.3 Geen DPIA verplicht

In de volgende gevallen is het niet verplicht om een DPIA uit te voeren:

1. 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;
2. wanneer de nationale toezichthouder heeft geoordeeld dat een DPIA niet verplicht is.

De Autoriteit Persoonsgegevens heeft geoordeeld dat een DPIA in ieder geval niet hoeft te worden uitgevoerd wanneer de gegevensverwerking waarschijnlijk geen hoog privacy risico oplevert of sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd. In het geval dat een keuze voor een bepaald ICT systeem en bepaalde beveiligingsmaatregelen getroffen wordt op het gebied van informatieveiligheid dan kan het wenselijk zijn om alsnog een DPIA uit te voeren. Zie de beslisboom in bijlage 2 om te beoordelen of een DPIA verplicht is. Als het IMG ervoor kiest om geen DPIA uit te voeren, moet deze keuze onderbouwd worden en vastgelegd worden.

2.4 De rol van de FG bij de DPIA

De Functionaris voor Gegevensbescherming (FG) van het IMG adviseert over de noodzaak van de DPIA en is altijd betrokken bij de beoordeling van de DPIA. De FG beoordeelt daarnaast de kwaliteit van en de bevindingen uit de DPIA en houdt toezicht op de uitvoering van de maatregelen die voortvloeien uit de DPIA.

2.5 Het herhalen van de DPIA

Het is belangrijk om de DPIA regelmatig opnieuw uit te voeren door het project of het proces opnieuw te beoordelen. Door deze herhaling wordt inzichtelijk of de resultaten van de DPIA nog actueel zijn.

De DPIA kan meermaals en op verschillende momenten worden uitgevoerd en geactualiseerd. Dit is voornamelijk het geval bij een wijziging van het voorstel waar ook een persoonsgegevensverwerking bij betrokken is. De wijziging wordt dan beoordeeld in samenhang met de bestaande verwerking.

Als de gegevensverwerking of de effecten daarvan veranderen, moet de DPIA worden geactualiseerd.

De Europese privacy toezichthouders geven als aanknopingspunt dat een DPIA elke drie jaar geëvalueerd moet worden en zo nodig (volledig) herhaald, gewijzigd of geactualiseerd.

Proceskader

3.1 Eigenaarschap

Beleid

Het bestuurslid (portefeuillehouder Informatiebeveiliging & Privacy) die verantwoordelijk is voor het beleid en de mogelijk daaruit voortvloeiende verplichtingen is formeel verantwoordelijk voor het uitvoeren van de DPIA. In de praktijk ligt die verantwoordelijkheid bij de proceseigenaar (lijnmanagement). Binnen het IMG wordt gebruik gemaakt van het concept 'three lines model' (zie het privacy beleid). In dit model is het lijnmanagement als eerste lijn verantwoordelijk voor de strategische visie, de risicobeheersing en ook voor het borgen van de aantoonbare naleving van wet- en regelgeving op het terrein van privacybescherming. De beheersing van privacy in projecten en nieuwe regelingen vallen hier ook onder.

Verwerkingen

Formeel is het IMG als verwerkingsverantwoordelijke, verantwoordelijk voor het uitvoeren van een DPIA. In de praktijk zal de bevoegdheid om te beslissen of en op welke wijze persoonsgegevens worden verwerkt zijn opgedragen aan proceseigenaar of gemandateerde (bijvoorbeeld een projectmanager) van een bedrijfsproces. De opgedragen functionaris is dan verantwoordelijk voor de uitvoering van een DPIA en de aan hen toegewezen maatregelen.

Daarnaast is de proceseigenaar verantwoordelijk voor het organiseren van de DPIA (zorgen dat iedereen om tafel komt), waardoor het DPIA proces voortvarend wordt opgepakt.

Wanneer meerdere proceseigenaren verantwoordelijk zijn voor de verwerking van persoonsgegevens dan moeten zij gezamenlijk zorgen voor de uitvoering van een DPIA. Zij kunnen deze verantwoordelijkheid ook neerleggen bij de projectmanager.

Indien een verwerker persoonsgegevens verwerkt voor het IMG, dat wil zeggen dat degene die persoonsgegevens verwerkt namens/in opdracht van het IMG, dan is deze verwerker niet verantwoordelijk voor de DPIA. Wel is de verwerker verplicht om het IMG bijstand te verlenen bij het uitvoeren van een DPIA.

3.2 Proces

De uitvoering van een DPIA bestaat uit de volgende processtappen.

1. De proceseigenaar dient alle relevante informatie over de verwerking te verzamelen. Hierbij kan gedacht worden aan procesbeschrijvingen, overeenkomsten, enz.
Verder is informatie nodig over onder andere:
 - Het project en de maatschappelijke context hiervan.
 - Wie zijn de belanghebbenden en welke eisen en wensen hebben zij?
 - Van wie worden er (persoons)gegevens verzameld?
 - Om wat voor soort (persoons)gegevens gaat het?
 - Op welke wijze gaan de persoonsgegevens verwerkt worden?
 - De verschillende systemen die gebruikt gaan worden om de gegevens te verwerken.
 - Wat zijn de doeleinden van de verwerking?
 - In hoeverre is het de bedoeling om de gegevens verder te gaan verwerken?
 - Worden met de gegevens persoonsprofielen gegenereerd?
2. Verder bespreekt de proceseigenaar de punten van het DPIA-model bij voorkeur in groepsverband, waar diverse relevante expertises deel van uitmaken. Betrokkenheid van meerdere personen met verschillende achtergronden en expertises – denk aan expertise op het gebied van het betreffende beleidsterrein, regelgeving, (informatie)beveiliging, archivering en ICT resulteert in een betere DPIA. Denk hierbij onder andere aan specialisten op het gebied van techniek (functioneel beheerders, key-users, i-adviseurs), bedrijfsvoering (DIV medewerker, contractadviseur, ISO/CISO, juridisch adviseur), beleidsadviseurs en uitvoering.

Voor het *uitvoeren* van een DPIA is in ieder geval een Privacy Officer van IMG die ondersteuning biedt bij de juridische (risico)analyse van de DPIA (conform privacy beleid) betrokken. Verder kan het wenselijk zijn om naast betrokken medewerkers van het betreffende project iemand van buiten het project te betrekken die inhoudelijke kennis kan toevoegen aan het opstellen van de DPIA.

3. Consulteer waar nodig² belanghebbenden, de organisaties die hen vertegenwoordigen of andere belanghebbenden. 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. Neem in de DPIA op wat de geconsulteerden hebben geadviseerd en wat daarmee gedaan is.
4. Leg de bevindingen schriftelijk (digitaal) vast in een rapport (administratieplicht AVG). Het IMG maakt gebruik van een model voor het uitvoeren van de DPIA's. In deel II wordt dit model nader toegelicht. Na afronding van het invullen van de DPIA vragen dient de ingevulde template voorgelegd te worden aan de Privacy Officer. De Privacy Officer maakt een risico-inschatting en adviseert over maatregelen die getroffen kunnen worden om risico's te vermijden of verkleinen, over eventuele vervolgacties en resterende risico's waarvoor geen maatregelen getroffen (kunnen) worden.
5. De AVG verplicht tot het consulteren van de FG. Leg daarom het DPIA-model – nadat de Privacy Officer heeft geadviseerd - ter advisering voor aan de FG. Neem de overwegingen, conclusie en aanbevelingen van de FG op in de DPIA.
6. Wanneer uit de DPIA blijkt dat de verwerking een hoog risico oplevert en de verwerkingsverantwoordelijke er niet in slaagt om maatregelen te nemen om dat (rest)risico te beperken tot een acceptabel niveau, moet de Autoriteit Persoonsgegevens voorafgaande aan de voorgenomen verwerking worden geraadpleegd. Volgens de Europese privacy toezichthouders is sprake van een onacceptabel hoog (rest)risico wanneer de betrokkene getroffen wordt door significante of onomkeerbare gevolgen die hij mogelijk niet te boven komt of als de kans daarop aanzienlijk is.

Voor het schriftelijk advies van de Autoriteit Persoonsgegevens over een voorgenomen verwerking moet rekening gehouden worden met een termijn van acht weken. Die termijn kan naar gelang de complexiteit van de voorgenomen verwerking met zes weken worden verlengd. Het advies van de AP wordt doorgestuurd naar de FG.

7. Na volledige invulling van het DPIA-model en zo nodig voorafgaande raadpleging door de Autoriteit Persoonsgegevens legt proceseigenaar de DPIA-rapportage en eventueel het schriftelijke advies van de Autoriteit Persoonsgegevens, vergezeld van een voorstel over te treffen maatregelen en een planning waarbinnen deze geïmplementeerd zullen worden, voor aan het Management Team (MT). Het MT besluit of en welke maatregelen worden getroffen en binnen welke termijn implementatie plaatsvindt.
8. Stuur het definitieve DPIA-rapport naar alle personen en/of organisaties die betrokken zijn geweest bij het opstellen daarvan, tenzij regels met betrekking tot geheimhouding daaraan in de weg staan. Vraag hiervoor de Privacy Officer om advies.
9. Registreer en leg vast. De proceseigenaar zorgt ervoor dat alle beschikbare documentatie vastgelegd worden in het archief van het IMG. Het betreft in ieder geval de volgende documentatie:
 - De ingevulde DPIA-vragenlijst inclusief bijgevoegde documenten;
 - Indien van toepassing: het separate advies van de FG;
 - Indien van toepassing: het schriftelijke advies van de Autoriteit Persoonsgegevens;
 - De adviesnota voor het MT inclusief bijlagen;
 - Het besluit van het verantwoordelijke bestuursorgaan;
 - Afschrift van de correspondentie naar personen die betrokken zijn geweest bij de uitvoering van de DPIA.

De proceseigenaar stuurt deze informatie ook naar de Privacy Officer. Deze registreert in het register van verwerkingen dat een DPIA is uitgevoerd met betrekking tot de betreffende verwerking van persoonsgegevens en de datum waarop deze is uitgevoerd.

De maatregelen uit de DPIA worden door de PO opgenomen in een maatregelen monitor.

² Hier is met name sprake van als een DPIA uitgevoerd wordt op een verwerking die onder het maatschappelijke vergrootglas ligt, en wanneer een grondige DPIA op maat plaatsvindt (bijv. de OR bij DPIA's op verwerkingen van medewerkers, cliëntenraden bij risicovolle verwerkingen van cliënten of bij risicovolle verwerkingen waarbij persoonsgegevens onderling worden gedeeld)

3. DPIA

De DPIA bestaat in de hoofdlijnen uit twee analyses, namelijk een analyse van de gegevensverwerking en een risicoanalyse met de analyse van de bijbehorende maatregelen. De twee analyses is onder te verdelen in vier onderdelen met 17 punten. In deel II wordt het DPIA-model met de vier onderdelen en 17 punten nader toegelicht.

De DPIA begint met een gegevensverwerkingsanalyse. Dit is een systematische beschrijving van de onderzochte projecten of processen. Dit is een feitelijke beschrijving van de betrokken systemen, partijen en persoonsgegevens. Na de gegevensverwerkingsanalyse volgt de risicoanalyse. Dit is een beoordeling van de risico's die voortkomen uit de voorgenomen verwerking gecombineerd met het opstellen van mitigerende maatregelen. Risico's worden afgewogen door de kans op het intreden van het risico te vermenigvuldigen met de impact. De impact is de ernst van de schade die wordt aangericht. Aan de hand van de bepaalde risico's worden passende maatregelen genomen om de risico's te beperken, dit is het mitigeren van risico's. Het risico dat overblijft na het nemen van maatregelen is het restrisico.

In acht onderdelen worden de gegevensverwerkingsanalyse en de risicoanalyse uitgevoerd:

1. Een beschrijving van het proces of het project waarin de persoonsgegevens verwerkt worden. Dit is een algemene beschrijving van het proces, de gebruikte systemen en de gegevensstromen binnen het IMG. Dit onderdeel bepaalt de scope van de DPIA.
2. Een opsomming van de persoonsgegevens die verwerkt worden. Dit bevat een analyse van de categorieën van persoonsgegevens die verwerkt worden binnen het IMG. Deze analyse moet in overeenstemming zijn met het verwerkingsregister.
3. Een beoordeling van de verwerkingsdoeleinden. In dit onderdeel worden de verwerkingsdoeleinden gespecificeerd, dit is verplicht in het kader van de beoordeling van de rechtmatigheid van de voorgenomen verwerking.
4. Een analyse van de betrokken partijen. Hierin wordt onderzocht welke partijen betrokken zijn bij de verwerking. Dit zijn bijvoorbeeld (gezamenlijk) verwerkingsverantwoordelijken, verwerkers en derden, maar ook betrokkenen.
5. Een analyse van de bewaartermijnen en de manier van archivering of vernietiging.
6. Een beoordeling van de rechtmatigheid van de verwerking. Het IMG moet hierbij ingaan op de rechtsgrond, de doelbinding, de noodzakelijkheid en de transparantie.
7. Een beoordeling van de risico's,
8. Een onderzoek naar passende maatregelen om de risico's te mitigeren.

Deel II: DPIA model Rijksoverheid



PIA-format.docx



Model-gegevensbe
schermingseffectber

Dit model wordt door het IMG gebruikt. Het DPIA-model bestaat uit 17 punten verspreid over de volgende vier onderdelen.

- A. Beschrijving kenmerken gegevensverwerkingen: een beschrijving van de voorgenomen verwerkingen en de verwerkingsdoeleinden;
- B. Beoordeling rechtmatigheid gegevensverwerkingen: een beoordeling van de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden;
- C. Beschrijving en beoordeling risico's voor betrokkenen: een beoordeling van de gevolgen en risico's van de voorgenomen verwerkingen voor de rechten en vrijheden van de betrokkenen. De voorgenomen verwerking kan een bepaald risico voor de betrokkene opleveren. In de DPIA moet daarom aandacht besteed worden aan welke gevolgen een bepaald risico heeft, wat de oorsprong van dergelijke risico's is, wat de waarschijnlijkheid (kans) is dat een gevolg zal intreden en wat de ernst (impact) van de gevolgen is;
- D. Beschrijving voorgenomen maatregelen: de voorgenomen maatregelen om deze gevolgen en risico's van de voorgenomen verwerkingen aan te pakken. Aan de hand van de risico's moet het IMG maatregelen nemen om de risico's te verkleinen. Maatregelen moeten vooral de beschikbaarheid, de integriteit en de vertrouwelijkheid van de persoonsgegevens beschermen. Dat houdt in dat de persoonsgegevens beschermd moeten worden tegen ongeoorloofde vernietiging, onrechtmatige wijziging of ongeoorloofde toegang.

A. Beschrijving kenmerken gegevensverwerkingen

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

1. Voorstel

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

Daarbij vormt het bepalen van de scope de basis van de DPIA. De scope bepaalt welke processen, functies, systemen en gegevens deel uitmaken van de te onderzoeken verwerking.

Daarom moet de DPIA aanvangen met een beschrijving van het voorstel waar de DPIA op ziet en de context waarbinnen deze verwerking plaatsvindt. Om de scope te bepalen kan het ook raadzaam zijn om expliciet te benoemen welke verwerkingen niet onder de scope van de DPIA zullen vallen.

In dit onderdeel moet het IMG aangeven:

- Voor welk project of proces een DPIA wordt uitgevoerd;
- Wat de voordelen van het proces zijn voor het IMG;
- Waarom een DPIA uitgevoerd moet worden voor het betreffende proces.

2. Persoonsgegevens (specificatie verwerking van persoonsgegevens)

Het IMG moet aangeven welke situatie centraal staat in de DPIA. Hierbij noteert het IMG welke persoonsgegevens daarbij worden verwerkt. Het is aan het IMG op welke manier wordt beschreven welke persoonsgegevens worden verwerkt. Voorbeelden van persoonsgegevens zijn: naam, adres, telefoonnummer, maar ook gezondheidsgegevens of andere bijzondere persoonsgegevens zoals het ras of politieke gezindheid. Het is voor het IMG van belang om te controleren of de lijst met gegevens juist en volledig is.

In dit onderdeel moet het IMG aangeven:

- Of en welke persoonsgegevens verwerkt worden;
- Hoe de gegevens verwerkt worden;

- Of de persoonsgegevens rechtstreeks bij de betrokkene worden verkregen of via een andere weg;
- Van welke categorieën van betrokkenen gegevens verwerkt worden en hierbij duidelijk aangeven of er sprake is van kwetsbare betrokkenen;
- Van hoeveel betrokkenen gegevens worden verwerkt;
- Of er gewone, bijzondere of strafrechtelijke gegevens verwerkt worden;
- Als er bijzondere persoonsgegevens verwerkt worden, welke uitzonderingsgrond op het verwerkingsverbod van toepassing is;
- Of er gezien het aantal betrokkenen en/of de hoeveelheid gegevens, sprake is van een grootschalige verwerking.

3. Gegevensverwerkingen

Geef alle voorgenumen gegevensverwerkingen weer.

In dit onderdeel moet het IMG aangeven:

- Welke verwerkingen relevant zijn voor het IMG;
- Hoe de gegevensverwerking verloopt.

4. Verwerkingsdoeleinden

Het IMG mag persoonsgegevens alleen gebruiken voor het doel waarvoor ze zijn verzameld of voor doeleinden die daarmee verenigbaar zijn. Het IMG moet daarom het doel van elke verwerking zo duidelijk en specifiek mogelijk formuleren.

In dit onderdeel moet het IMG aangeven:

- Wat het doel van het project of het proces is;
- Wat zijn de voordelen van het proces voor het IMG;
- Wat is het juridische kader van de verwerking;
- Wat het beleidsmatige-/normenkader van de verwerking is;
- Of het doel van de verwerking duidelijk is vastgesteld.

5. Betrokken partijen (specificatie partijen en betrokkenen)

Het IMG moet hier overzichtelijk weergeven of, en zo ja welke, verwerkers, subverwerkers of zelfs gezamenlijk verwerkingsverantwoordelijken betrokken zijn bij de verwerking. Op het moment dat het IMG leveranciers of afnemers bij de verwerking betreft, moeten met deze partijen goede afspraken gemaakt worden over de omgang met persoonsgegevens. Om te kunnen bepalen wat met partijen afgesproken moet worden, moet het IMG inzichtelijk hebben welke partijen bij de verwerking betrokken zijn en wat de rol van deze partijen is bij de specifieke verwerking.

In dit onderdeel moet het IMG aangeven:

- Of er behalve het IMG meer partijen betrokken zijn in de rol van verwerkingsverantwoordelijke;
- Daarnaast de rollen van verwerker, verstrekker en ontvanger per gegevensverwerking in beeld brengen;
- Tevens benoemen welke functionarissen binnen het IMG toegang krijgen tot welke persoonsgegevens (zie autorisaties en toegangscontrole).

Afspraken met derde partijen

Het IMG is verwerkingsverantwoordelijke bij de verwerking en bepaalt dus het doel en de middelen van de verwerking. Het IMG betreft hier mogelijk ook verwerkers bij. Met deze verwerkers moeten afspraken worden gemaakt over de verwerking. Dit kan door middel van een verwerkersovereenkomst. De verwerkersovereenkomst moet aan [een aantal eisen](#) voldoen.

In dit onderdeel moet het IMG aangeven:

- Of er verwerkers betrokken zijn bij de verwerking en
- Of met elke verwerker een verwerkersovereenkomst is afgesloten die aan de wettelijke eisen voldoet.

6. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenumen gegevensverwerkingen.

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

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Op het moment dat het IMG persoonsgegevens doorgeeft naar landen buiten de EER, omdat bijvoorbeeld gebruik wordt gemaakt van bijvoorbeeld clouddiensten, moet het IMG passende waarborgen verzekeren voor de doorgifte. In deze landen buiten de EER geldt namelijk de AVG niet.

In dit onderdeel moet het IMG aangeven:

- Worden er alleen in Nederland gegevens verwerkt?

Toelichting: Beschrijf waar de gegevensverwerking plaatsvindt. Benoem de locaties en de landen waar dit gebeurt. Geef aan of dit alleen in Nederland is of ook in het buitenland.

Uitleg: Om een duidelijk beeld te krijgen van de gegevensverwerking is het van belang om te weten waar de persoonsgegevens worden verwerkt, op welke locatie en in welk land. Het gaat hier dus om fysieke locaties. De verwerking van gegevens buiten de EER is namelijk aan strenge eisen gebonden. Zie in de opvolgende vraag of de gegevensverwerking in het buitenland aan de voorwaarden voldoet.

- Worden in andere landen dan Nederland gegevens verwerkt?

Toelichting: Geef aan of in andere landen dan Nederland gegevens verwerkt worden voor het systeem. Als dit het geval is, benoem dan de locaties en landen waar de gegevensverwerkingen plaatsvinden.

Uitleg: De locaties waar de verwerkingen plaatsvinden kunnen aanvullende privacy risico's met zich brengen en daarom moeten sommige verwerkingen voldoen aan strengere regels en aanvullende maatregelen. De AVG bepaalt dat gegevensverwerkingen buiten de Europese Unie, naar 'derde landen', alleen onder bepaalde omstandigheden toegestaan zijn. Dat komt omdat de doorgifte naar dit derde land [maar in vier gevallen toegestaan is](#).

- Worden op rechtmatige wijze gegevens doorgegeven naar buiten de EER?

Toelichting: Beschrijf voor de gevallen waarin gegevens buiten de EER worden verwerkt op welke grond dit gebeurt en of de gegevensverwerking dus is toegestaan.

Uitleg: Zoals hierboven is beschreven stelt de AVG eisen aan de verwerking van persoonsgegevens buiten de EER, dit zijn derde landen. Derde landen zijn alle landen buiten de EU, behalve Noorwegen, Liechtenstein en IJsland. Om in het derde land gegevens te verwerken, moet de doorgifte ervan op een rechtmatige wijze plaatsvinden.

In vier gevallen is het mogelijk om persoonsgegevens door te geven naar een derde land;

1. Een **adequaateheidsbesluit**: als de Europese Commissie vindt dat een derde land in de nationale wetgeving een passend niveau van gegevensbescherming biedt, dat vergelijkbaar is met de AVG, kan het een adequaatheidsbesluit nemen en mogen persoonsgegevens buiten de EER verwerkt worden (bijvoorbeeld Israël, Japan, het VK of Zwitserland)
2. **Passende waarborgen**: Als er geen adequaatheidsbesluit is, kan door middel van een modelcontract of een goedgekeurde gedragscode of certificeringsmechanismen. Een modelcontract, ook wel standard contractual clauses, wordt door de Europese Commissie vastgesteld. Een dergelijk modelcontract zorgt ervoor dat een verwerkingsverantwoordelijke zelf niet een contract op hoeft te stellen. Ook is het mogelijk om via goedgekeurde modelcontracten en certificeringsmechanismen gegevens te verwerken in een derde land. Een extra voorwaarde hieraan is echter wel dat het IMG bindende en afdwingbare toezeggingen heeft dat de partij in het derde land deze juiste waarborgen toepast;
3. **Binding Corporate Rules (BCR)**: Binding corporate rules zijn policies die gelden binnen organisaties voor alle werknemers en entiteiten binnen het concern, inclusief de Europese vestigingen;
4. **Specifieke uitzonderingen**: Als alle drie bovenstaande opties niet van toepassing zijn, is het nog mogelijk dat sprake is van een specifieke uitzondering. Dit kan de uitdrukkelijke toestemming van de betrokkene zijn, dat de verwerking noodzakelijk is voor de uitvoering van een overeenkomst die betrekking heeft op de betrokkene of door de betrokkene wordt gesloten, of het noodzakelijk is wegens gewichtige redenen van algemeen belang, een rechtsvordering of van vitaal belang is.

8. Technieken en methoden van de gegevensverwerkingen

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

In dit onderdeel moet het IMG aangeven:

- Of er sprake is van nieuwe technologieën, geautomatiseerde besluitvorming en/of profilering;
- Welke negatieve gevolgen de gegevensverwerking kan hebben voor de rechten en vrijheden van betrokkenen en waar deze gevolgen vandaan komen;

9. Juridische en beleidsmatig kader

In dit onderdeel moet het IMG aangeven:

- Wat is het juridische kader van de verwerking?

Toelichting: Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

Uitleg: Naast of in de plaats van de AVG kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, reguleren of beperken.

10. Bewaartermijnen (Opslagbeperking)

Het IMG heeft de taak om ervoor te zorgen dat de gegevens niet langer dan noodzakelijk bewaard worden. Het IMG moet daarom voor alle persoonsgegevens aangeven welke bewaartermijn wordt gehanteerd en waarom dit noodzakelijk is om de gegevens voor deze termijn te bewaren. Het IMG moet hierbij uitgaan van het **noodzakelijkheidsbeginsel**, dus als de gegevens niet langer noodzakelijk bewaard moeten worden, moet het IMG ze verwijderen. Voor een aantal persoonsgegevens geldt in specifieke situaties dat er wettelijke bewaartermijnen voor vastgelegd zijn. Het IMG moet daarom voor alle persoonsgegevens specifiek aangeven wat de bewaartermijn is die wordt gehanteerd en daarnaast ook hoe het IMG erop toeziet hoe de gegevens na die termijn ook daadwerkelijk verwijderd worden.

In dit onderdeel moet het IMG aangeven:

- Of er voor elke categorie van persoonsgegevens een minimale en maximale bewaartermijn is bepaald en wat deze termijnen dan zijn;
- Waarom het voor elke categorie van persoonsgegevens noodzakelijk is om deze gegevens voor de bepaalde termijn te bewaren;
- Of de vastgestelde bewaartermijnen en de wijze van naleving daarvan in overeenstemming zijn met het door het IMG vastgestelde beleid;
- Of, in het geval dat nodig is, de gegevens op een juiste manier gearchiveerd worden;
- Welke maatregelen zijn genomen om toe te zien op de naleving van de bewaartermijnen en om de gegevens na het verstrijken van de bewaartermijn ook daadwerkelijk te verwijderen en
- Welke afspraken met (sub)verwerkers zijn gemaakt over het verwijderen of teruggeven van de persoonsgegevens na het verstrijken van de bewaartermijn.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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

11. Rechtsgrond (Wettelijke grondslag)

De AVG eist dat de gegevensverwerking plaatsvindt op een rechtmatige, behoorlijke en transparante wijze. De gegevensverwerking moet gebaseerd zijn op een wettelijke grondslag om te kunnen spreken van een rechtmatige verwerking. Het IMG moet in dit onderdeel aantonen op welke grondslag het zich baseert voor de verwerking.

In dit onderdeel moet het IMG aangeven:

- Is de verwerking op een rechtmatige rechtsgrond gebaseerd?

Toelichting: Geef aan wat de wettelijke basis is om de gegevensverwerking rechtmatig te laten zijn. Beschrijf dit per verwerking. Leg daarnaast ook uit waarom dit de juiste rechtsgrondslag is.

Uitleg: De AVG gaat er van uit dat persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Om de verwerking rechtmatig te laten zijn, moet de verwerking gebaseerd worden op tenminste één van de zes limitatief omschreven rechtsgronden;

1. Het IMG heeft **toestemming** van de betrokkene, dit is de persoon om wie de verwerking draait. De rechtsgrondslag toestemming is aan nadere eisen gebonden.
2. Het is noodzakelijk om gegevens te verwerken voor de **uitvoering van een overeenkomst**: Het IMG mag gegevens verwerken op het moment dat er een overeenkomst met iemand is en hiervoor het verwerken van persoonsgegevens noodzakelijk is.
3. Het is noodzakelijk omdat het IMG dit **wettelijk verplicht** is: Bij deze rechtsgrondslag hoeft het niet specifiek uit de wet te blijken dat het IMG persoonsgegevens moet verwerken. De verplichting kan ook ruimer geformuleerd worden. Het IMG moet zelf bepalen of de verwerking noodzakelijk is om aan de verplichting te voldoen.
4. Het is noodzakelijk omdat het IMG **vitale belangen** moet beschermen: Van vitale belangen is sprake als het belang essentieel is voor iemands leven of gezondheid, en die persoon niet om toestemming gevraagd kan worden.
5. Het is noodzakelijk omdat het gaat om een **taak van algemeen belang** of **openbaar gezag**: Een beroep op deze rechtsgrondslag is alleen mogelijk indien het IMG een publieke taak uitoefent voor het algemeen belang of openbaar gezag. In de wet moet de taak zijn vastgelegd en de taak moet relevant zijn voor het IMG.
6. Het is noodzakelijk om een **gerechtvaardigd belang** te behartigen: Op het moment dat het IMG een belang heeft dat de in de samenleving als dusdanig zwaar wordt gezien, dat het mag worden afgewogen tegen het grondrecht van de bescherming tegen een inbreuk op de privacy van de betrokkene. Het IMG moet de beide belangen afwegen en mag zich op deze rechtsgrond beroepen op het moment dat het belang van het IMG zwaarder weegt.

De gegevensverwerking moet bovendien dus ook noodzakelijk zijn. Of hier sprake van is, kan worden beoordeeld aan de hand van het volgende subonderdeel, namelijk de noodzakelijkheid en evenredigheid.

12. Bijzondere persoonsgegevens

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

In dit onderdeel moet het IMG aangeven:

- Worden er bijzondere categorieën van persoonsgegevens verwerkt?

Toelichting: Benoem of er bijzondere categorieën van persoonsgegevens verwerkt worden. Als dat het geval is, benoem dan ook welke categorieën dit zijn.

Uitleg: Bijzondere categorieën van persoonsgegevens zijn kwetsbare persoonsgegevens en een verhoogde kans op misbruik kennen. Dit heeft een grote impact op de betrokkene en dus vereist de verwerking betere beveiliging dan de verwerking van gewone persoonsgegevens. De verwerking van dergelijke gegevens is daarom in beginsel verboden, tenzij er een specifieke uitzondering van toepassing is of de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking. Zie voor deze opheffingsgronden vraag 33.

De categorieën van bijzondere persoonsgegevens kunnen limitatief worden opgesomd. Dit zijn namelijk gegevens over;

- 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.

13. Doelbinding

Op het moment dat de gegevens voor een ander doel van oorspronkelijk worden verwerkt, moet het IMG beoordelen of deze gegevensverwerking verenigbaar is met het oorspronkelijke doel.

In dit onderdeel moet het IMG aangeven:

- Worden de persoonsgegevens verwerkt voor een ander doel dan waarvoor ze in de eerste instantie verkregen zijn?

Toelichting: Geef aan of de persoonsgegevens voor een ander doel worden verwerkt dan waar ze oorspronkelijk voor verzameld zijn. Beargumenteer waarom de verwerking alsnog wel verenigbaar is met het oorspronkelijke doel.

Uitleg: De AVG heeft als uitgangspunt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde verwerkingsdoeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die verwerkingsdoeleinden onverenigbare wijze, dit is het [doelbindingsbeginsel](#). Als de persoonsgegevens wel voor een ander doel worden verwerkt dan waarvoor ze oorspronkelijk verzameld zijn, moet deze verwerking wel verenigbaar zijn met het oorspronkelijke doel.

14. Noodzaak en evenredigheid (Noodzakelijkheid)

Om de rechtmatigheid van de gegevensverwerking te beoordelen is het vereist dat de gegevens en de verwerkingen daarvan noodzakelijk en evenredig zijn in relatie tot het beoogde doel van de verwerking.

In dit onderdeel moet het IMG aangeven:

- Is het verwerken van de gegevens noodzakelijk om het hierboven beschreven doel te bereiken, of kan zonder de gegevens hetzelfde resultaat worden bereikt?

Toelichting: Leg uit waarom de verzamelde gegevens noodzakelijk zijn voor de verwerkingsdoeleinden. Beoordeel of de verwerking proportioneel is ten opzichte van de inbreuk op de bescherming van de persoonsgegevens van de betrokkene.

Uitleg: Bij proportionaliteit moet worden bekeken of het doel van de gegevensverwerking in verhouding staat tot de mogelijke inbreuk van die gegevensverwerking op de privacy van de betrokkene. Hierbij is het vooral relevant of de verwerking effectief is om het beoogde doel te bereiken.

Bij subsidiariteit moet worden bekeken of de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, kan worden verwezenlijkt. Kan hetzelfde resultaat van het verwerkingsdoel worden bereikt op het moment dat de gegevens op een andere manier verwerkt worden.

15. Rechten van de betrokkenen (Rechten van betrokkenen)

Om een eerlijke verwerking van persoonsgegevens te waarborgen hebben betrokkenen een aantal rechten. Het IMG moet het systeem zo hebben ingericht dat binnen één maand aan een dergelijk verzoek kan worden voldaan. Als het verzoek erg complex is, dient het IMG binnen één maand mede te delen dat het binnen maximaal twee maanden extra terugkomt op het verzoek van de betrokkene. De betrokkene heeft een recht op inzage, een recht op vergetelheid, een recht op rectificatie en aanvulling, een recht op dataportabiliteit, een recht op beperking van de verwerking, een recht op een menselijke blik bij besluiten, het recht om bezwaar te maken en een recht op duidelijke informatie.

Het IMG heeft een intern proces over hoe het omgaat met de rechten van betrokkenen (proces AVG verzoek). Intern moet deze proces worden gevolgd, zodat op elk verzoek op dezelfde wijze kan worden gereageerd. Het IMG moet daarnaast ook met alle verwerkers afspraken maken over de wijze waarop verwerkers moeten omgaan met de verzoeken van betrokkenen. Het is gebruikelijk om de afspraak te maken dat de verwerker aan het IMG doorgeeft dat er een verzoek is binnengekomen, maar dat het IMG uitvoering geeft aan het verzoek.

In dit onderdeel moet het IMG aangeven:

- Of invulling wordt gegeven aan de rechten van betrokkenen en op welke manier dit gebeurt.

Informatieplicht

Het IMG moet de betrokkenen informeren over de gegevensverwerking, zodat de betrokkene weet wat er met de gegevens gebeurt en waarom het IMG deze gegevens verwerkt.

In dit onderdeel moet het IMG aangeven:

- Of het IMG een beroep kan doen op de uitzondering op de informatieplicht;
- Of en op welke wijze betrokkenen geïnformeerd worden over de verwerking;
- Waarover de betrokkenen worden geïnformeerd;
- Of er een privacyverklaring is waarin betrokkenen worden gewezen op de verwerking en
- Of er een interne privacyverklaring is waarin medewerkers worden gewezen op de verwerking.

C. Beschrijving en beoordeling risico's voor betrokkenen.

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

16. Risico's

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

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

Na het uitvoeren van de DPIA blijven er mogelijk nog restrisico's achter. Het IMG moet beoordelen of deze risico's acceptabel zijn en waarom het niet mogelijk was om het vastgestelde risico volledig af te dekken. Daarnaast moet het IMG de restrisico's periodiek controleren en beoordelen of het nog steeds geaccepteerd is of dat er nieuwe maatregelen genomen moeten worden.

D. Beschrijving voorgenomen maatregelen

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

17. Maatregelen

Juistheid

De juistheid van de gegevens houdt in dat de persoonsgegevens die verwerkt worden, correct en actueel zijn. De persoonsgegevens die dat niet (meer) zijn, moeten worden gewijzigd of gewist. Het IMG moet in de DPIA aantonen dat het maatregelen heeft genomen om de juistheid van de gegevens te waarborgen en welke maatregelen dit zijn.

In dit onderdeel moet het IMG aangeven:

- Of gewaarborgd is dat de gebruikte persoonsgegevens juist en up-to-date zijn;
- Welke waarborgen worden gebruikt om de juistheid van de gegevens te verzekeren.

Beveiligingsmaatregelen

Het IMG is verplicht om persoonsgegevens op een veilige manier te verwerken, dit kan door middel van het treffen van 'passende technische en organisatorische maatregelen', die op het risico van de verwerking afgestemd zijn. De AVG geeft geen lijst met maatregelen, het is aan het IMG om te bepalen welke maatregelen in het specifieke geval van de verwerking genomen moeten worden.

In dit onderdeel moet het IMG aangeven:

- Welke negatieve gevolgen de gegevensverwerking kan hebben voor de rechten en vrijheden van betrokkenen en waar deze gevolgen vandaan komen;
- Hoe waarschijnlijk het is dat de negatieve gevolgen intreden en wat de impact van deze gevolgen is;
- Welke maatregelen het heeft genomen om de verwerking te beveiligen en wat het (gewenste) resultaat van die maatregelen is;
- Welke maatregelen het verwerkers oplegt om de verwerking te beveiligen;
- Of de genomen maatregelen periodiek gecontroleerd worden op passendheid.

Autorisaties en toegangscontrole

Een belangrijk onderdeel van de beveiligingsmaatregelen zijn een autorisatiebeleid en toegangscontrole. Op deze manier kan het IMG de toegang tot een minimum beperken.

In dit onderdeel moet het IMG aangeven:

- Of er een toegangsbeveiligingsbeleid is opgesteld;
- Wie (in welke functie) toegang heeft tot welke gegevens en waarom deze toegang nodig is.

Controle

Het IMG moet de genomen maatregelen op gezette tijdstippen testen, beoordelen en evalueren op doeltreffendheid. Dit zorgt ervoor dat de maatregelen op alle momenten tijdens de verwerking passend blijven. Het IMG moet daarom een plan-do-check-act-cyclus implementeren, waardoor de maatregelen continu gecontroleerd worden.

Bijlage 1: Begrippenkader

Autoriteit Persoonsgegevens: De onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

AVG: Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PbEU 2016, L 119)

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon over wie persoonsgegevens worden verwerkt.

Europese privacy toezichthouders: Alle nationale privacy toezichthouders uit de Europese Unie werken samen bij hun toezicht op de AVG in de European Data Protection Board (EDPB). De EDPB neemt besluiten en publiceert regelmatig werkdocumenten en opinies over de toepassing van de AVG en andere privacy kwesties. Taken en bevoegdheden zijn onder meer: het uitbrengen van guidelines, het nemen van (bindende) besluiten en het bevorderen van een uniforme toepassing van de principes uit de AVG in alle lidstaten.

Functionaris voor de Gegevensbescherming (FG): is een door een organisatie aangestelde privacy toezichthouder. Zijn positie, kwalificaties en taken zijn bij wet geregeld. De belangrijkste taken zijn: (1) toezien op naleving van de privacywetgeving en intern privacy beleid, (2) informeren en adviseren van de bestuursorganen, directie, MT en medewerkers over naleving van privacywetgeving, (3) onderhouden van de contacten met de Autoriteit Persoonsgegevens.

Gevoelige persoonsgegevens/ gevoelige informatie: gegevens die naar hun aard gevoelig zijn en daarom extra bescherming behoeven. Hierbij kan gedacht worden aan inloggegevens, financiële gegevens, gegevens waarmee identiteitsfraude gepleegd kan worden, gegevens die onder een wettelijke geheimhoudingsplicht vallen etc.

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Privacy by design: houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. En dat u de gegevens niet langer bewaart dan nodig is voor het doel van de verwerking.

Privacy by default: het nemen van technische en organisatorische maatregelen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

Verantwoordingsplicht: De plicht om aan te tonen dat een organisatie aan de AVG voldoet. De verplichte maatregelen die de AVG concreet noemt zijn: het bijhouden van een verwerkingsregister, het uitvoeren van DPIA's op verwerkingen die waarschijnlijk een hoog privacy risico inhouden, het bijhouden van een register van datalekken en het aantonen dat betrokkenen daadwerkelijk toestemming hebben gegeven voor een verwerking als deze gebaseerd is op de grondslag "toestemming" en het goed kunnen onderbouwen waarom ervoor gekozen is om geen FG aan te stellen als onduidelijk is of hiervoor een verplichting geldt.

Verwerker: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerking: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen,

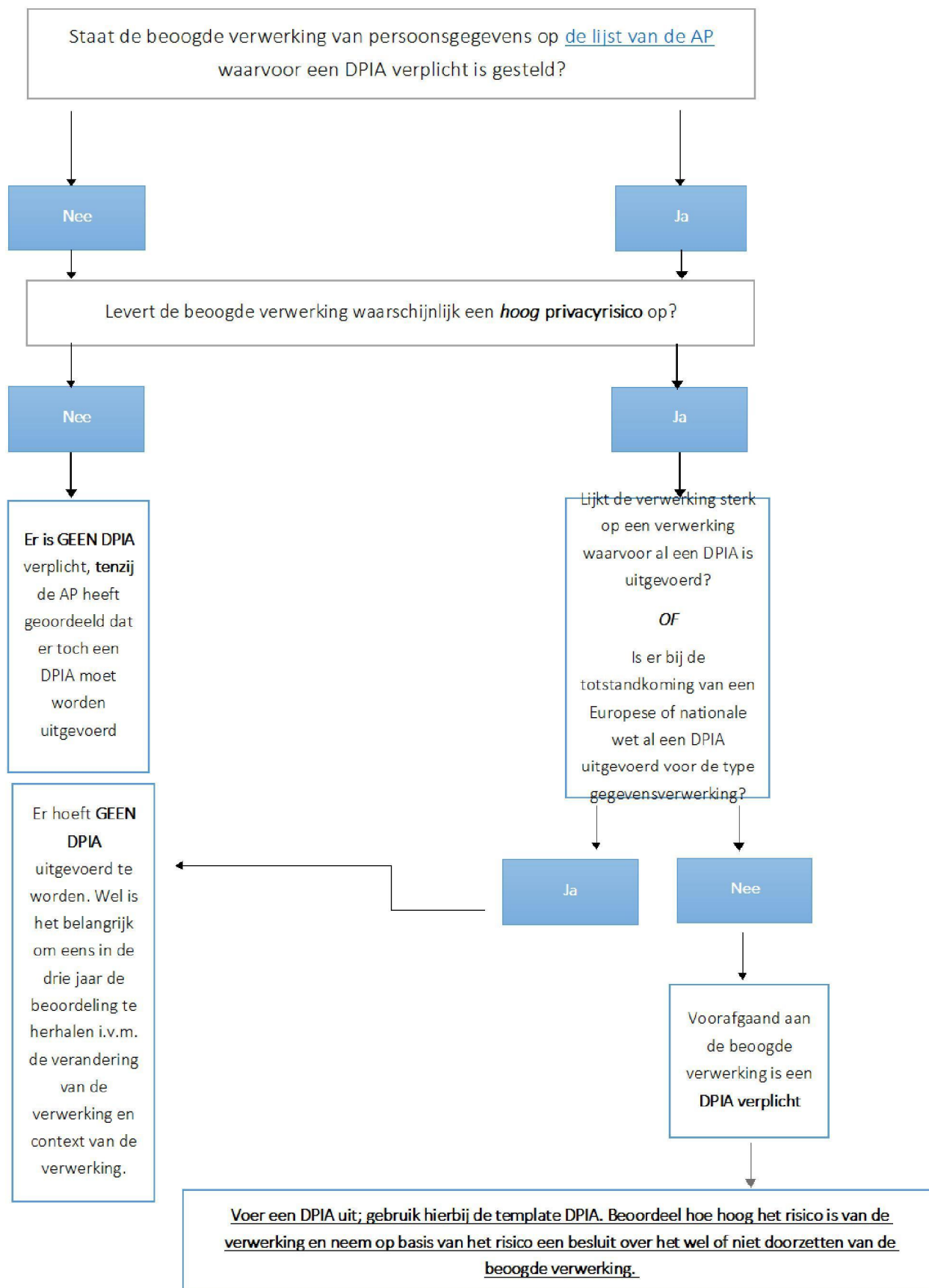
raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsregister: Het IMG is verplicht een register bij te houden dat voortdurend bijgewerkt wordt en informatie bevat over de verwerking, zoals contactgegevens van de verantwoordelijken en verwerkers, de doeleinden van de verwerking en categorieën van persoonsgegevens.

Verwerkingsverantwoordelijke: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Voorafgaande raadpleging: Als uit een DPIA naar voren komt dat een beoogde verwerking een hoog risico oplevert, en er geen maatregelen gevonden worden om dit risico te beperken moet een organisatie met de Autoriteit Persoonsgegevens overleggen voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. Bij een voorafgaande raadpleging geeft de Autoriteit Persoonsgegevens advies hoe de risico's van een voorgenomen verwerking beperkt kunnen worden. Als deze maatregelen uitgevoerd worden, mag met de verwerking gestart worden. Het kan ook dat de Autoriteit Persoonsgegevens adviseert om helemaal van de verwerking af te zien. Soms is een advies van de Autoriteit Persoonsgegevens niet nodig, bijvoorbeeld omdat de risico's toch voldoende blijken te zijn afgedekt. In dat geval mag gelijk met de verwerking gestart worden.

Bijlage 2: Beslisboom DPIA



Bijlage 3: PreDPIA model

Vragenlijst Persoonsgegevens PreDPIA

Lijst 1: Verwerkingen waarvoor een DPIA verplicht is. De AP heeft een lijst uitgegeven van verwerkingen waarvoor de DPIA verplicht is, indien op deze lijst één van de antwoorden JA is, dan hoeft deel 2 niet meer te worden ingevuld. En kan men direct beginnen met de DPIA.

	Omschrijving AP	ja/nee	Argumentatie
1	Heimelijk onderzoek : Grootschalige en/of systematische verwerkingen van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder dat de betrokkene daarvan vooraf op de hoogte te stellen.	Nee	
2	Zwarte lijsten : Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag (artikel 33, lid 4, aanhef en onder c, UAVG) of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.	Nee	
3	Fraudebestrijding : Grootschalige en/of systematische verwerkingen van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.	Nee	
4	Creditscores : Grootschalige en/of systematische gegevensverwerkingen die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.	Nee	
5	Financiële situatie : Grootschalige en/of systematische verwerkingen van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.	Nee	
6	Genetische persoonsgegevens : Grootschalige en/of systematische verwerkingen van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.	Nee	
7	Gezondheidsgegevens : Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal) onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.	Nee	
8	Samenwerkingsverbanden : Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin het IMG met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid of financiële situatie) met elkaar uitwisselen.	Nee	

9	Cameratoezicht : Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.	Nee	
10	Flexibel cameratoezicht : Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.	Nee	
11	Controle werknemers : Grootschalige en/of systematische verwerking van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding.	Nee	
12	Locatiegegevens : Grootschalige en/of systematische verwerking van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.	Nee	
13	Communicatiegegevens : Grootschalige en /of systematische verwerking van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.	Nee	
14	Internet of things : Grootschalige en/of systematische verwerkingen door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.	Nee	
15	Profilering : Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.	Nee	
16	Observatie en beïnvloeding van gedrag : Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.	Nee	

Lijst 2: Algemene DPIA vragen. Tel de waardes van de gekozen antwoorden bij elkaar op, alle waardes groter of gelijk aan 6 betekenen dat een DPIA moet worden uitgevoerd.

Algemene vragen m.b.t. doeleinden en doelbinding van de verwerking van persoonsgegevens		Keuze	Resultaat	Argumentatie (verplicht invullen)
	Resultaat blok 1, is een DPIA verplicht? (als hier een verwerking is gekozen waarvoor een DPIA verplicht is dan hoeven de onderstaande vragen niet meer beantwoord te worden)	Nee	0	
P1	Beoordelen van mensen op basis van persoonskenmerken Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.	Nee	0	
P2	Geautomatiseerde beslissingen Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.	Nee	0	
P3	Stelselmatige en grootschalige monitoring Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht.	Nee	0	
P4	Gevoelige gegevens Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG).	Nee	0	
P5	Grootschalige gegevensverwerkingen	Nee	0	
P6	Gekoppelde databases Het gaat hierbij om gegevensverzamelingen die aan	Nee	0	

	elkaar gekoppeld of met elkaar gecombineerd zijn.			
P7	Gegevens over kwetsbare personen Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens.	Nee	0	
P8	Gebruik van nieuwe technologieën De AVG is er duidelijk over dat een PIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacy risico's.	Nee	0	
p9	Doorgifte van persoonsgegevens buiten de EU De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Buiten de EU is het daarom niet zeker dat een land voldoende bescherming biedt.	Nee	0	
P10	Blokking van een recht, dienst of contract Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.	Nee	0	

Handboek Privacy voor alle medewerkers IMG

Instituut
Mijnbouwschade
Groningen



Eigenaar: 5.1.2e

Datum : 20 mei 2025

Versie : D 1.0

Revisie lijst

Versie	Wijzigingen t.o.v. vorige versie	Author	Date
C 0.1	1 ^e opzet	5.1.2e	14-01-2025
C 0.2	Revisie Privacy team	Privacy team	01-02-2025
C 0.3	Aanpassingen n.a.v. Revisie	5.1.2e	03-02-2025
D 1.0	Definitieve versie	5.1.2e	20-05-2025

Behorend bij:

Procesbeschrijving:	N.v.t.
Wetgeving/Regeling	Algemene verordening gegevensbescherming
Afdeling:	Alle afdelingen binnen het IMG
Handleidingen:	N.v.t.
Systemen:	Systeem overstijgend
Overige documenten:	Alle andere documenten die op de T-schijf zijn gepubliceerd
Informatie bronnen:	https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679
Bijlagen:	Bijlage 1: begrippen Bijlage 2: beslisboom persoonsgegevens
Activiteitnaam:	Bij het uitvoeren van de dagelijkse werkzaamheden dient rekening gehouden te worden met dit handboek
Roepnaam functie:	Alle interne en externe medewerkers van het IMG
Uit te voeren handelingen:	Dit Privacy handboek is een leidraad voor hoe binnen het IMG wordt omgegaan met privacy gerelateerde gegevens. Dit worden persoonsgegevens genoemd. Dit handboek is door de Privacy Officers van het IMG opgesteld als handvat bij het gebruik van persoonsgegevens.

Inhoudsopgave

1.	Inleiding.....	4
2.	Intern gebruik van gegevens.....	5
2.1	Wat zijn persoonsgegevens?.....	5
2.2	Verwerken van gegevens.....	5
2.3	Soorten persoonsgegevens.....	7
2.4	Doeleinden verwerken gegevens.....	8
2.5	Verzenden van gegevens.....	9
2.6	Bewaren van gegevens.....	9
3.	Datalekken.....	11
4.	Rechten van betrokkenen.....	12
5.	Overige documenten.....	13
5.1	Werkinstructie blurren.....	13
5.2	Privacy by Design/privacy by default.....	13
5.3	AI-beleid.....	13
5.4	Awareness.....	13
5.5	DPIA's.....	14
6.	FAQ.....	15
7.	Contact.....	18
8.	Bijlagen.....	19
8.1	Bijlage 1 – Begrippen.....	20
8.2	Bijlage 1 – Beslisboom persoonsgegevens.....	22

1. Inleiding

Dit Privacy handboek (intern privacybeleid) is een leidraad hoe binnen het Instituut Mijnbouwschade Groningen (hierna: het Instituut/het IMG/wij) wordt omgegaan met privacy gerelateerde gegevens. Dit worden persoonsgegevens genoemd. Dit handboek is door de Privacy Officers van het Instituut opgesteld als handvat bij het gebruik van persoonsgegevens.

Inhoud en gebruik

In dit handboek wordt uitgelegd wat persoonsgegevens zijn, welke regels er gelden bij het gebruik van deze gegevens en welke maatregelen onze medewerkers moeten en kunnen nemen bij het gebruik van deze gegevens. Het is belangrijk om dit handboek goed na te leven. Door dit handboek na te leven wordt de privacy van onze mensen (waaronder aanvragers, medewerkers en bezoekers van de websites) gewaarborgd. Het op een juiste manier verwerken van persoonsgegevens is ieders verantwoordelijkheid binnen het Instituut.

Houden wij ons niet aan dit handboek, dan bestaat er een kans dat gegevens van mensen bijvoorbeeld verloren raken en de privacy van hen hierdoor wordt geschonden. Als organisatie willen wij dit voorkomen. Houd je daarom altijd aan de regels van dit handboek wanneer je met persoonsgegevens werkt.

Wijzigingen

Dit handboek heeft een dynamisch karakter en kan van tijd tot tijd worden aangevuld of herzien. Dit kan naar aanleiding van veranderingen in onze organisatie, bedrijfsprocessen, aanpassingen van informatiesystemen of wetswijzigingen. Indien het handboek aangepast wordt, zullen wij dit laten weten.

Vragen?

Bij vragen over dit handboek of over privacy in het algemeen kan je terecht bij een van de Privacy Officers. De Privacy Officers zijn te bereiken via het volgende e-mailadres: privacy@schadedoormijnbouw.nl.

2. Intern gebruik van gegevens

2.1 Wat zijn persoonsgegevens?

Om duidelijk aan te geven hoe we binnen het Instituut omgaan met persoonsgegevens, is het belangrijk eerst goed voor ogen te hebben wat persoonsgegevens precies zijn.

Persoonsgegevens zijn de gegevens over een persoon die ervoor zorgen dat een persoon identificeerbaar is, of geïdentificeerd kan worden. Een persoonsgegeven kan direct of indirect naar een persoon herleiden.

Aan de hand van een naam of adres is gemakkelijk vast te stellen om welke persoon het gaat. Maar ook als er meerdere gegevens gecombineerd moeten worden om vast te stellen om wie het gaat, kan er sprake zijn van een persoonsgegeven. Zo kan een postcode of IP-adres naar een persoon herleid worden, zoals een medewerker of een aanvrager. Hier zijn echter wel aanvullende gegevens voor nodig, zoals bijvoorbeeld een huisnummer.

In onze systemen zijn vrijwel alle gegevens gekoppeld aan een dossier. Hierdoor is het eenvoudig te achterhalen bij welke persoon de gegevens horen. Daarom zijn de gegevens die gebruikt worden in onze systemen aan te merken als persoonsgegevens. Persoonsgegevens kunnen uiteraard ook gegevens van onze eigen medewerkers zijn.

Voorbeelden van veelgebruikte persoonsgegevens zijn:

- NAW-gegevens;
- telefoonnummer;
- e-mailadres;
- geslacht;
- geboortedatum;
- zaaknummer.

De persoon waarvan de persoonsgegevens zijn, wordt ook wel de 'betrokkene' genoemd. In dit handboek wordt de aanvrager vaak als voorbeeld genoemd. Dit handboek geldt echter voor *alle* betrokkenen, dus ook medewerkers of andere personen wiens persoonsgegevens bij het Instituut terecht zijn gekomen.

2.2 Verwerken van gegevens

Het verwerken van persoonsgegevens is alles wat je doet met persoonsgegevens. Er zijn wettelijke rechten en plichten verbonden aan het verwerken van persoonsgegevens. Onder verwerken vallen alle handelingen die met persoonsgegevens worden verricht zoals:

- het opslaan van gegevens;
- het verwijderen van gegevens;
- het raadplegen van gegevens;
- het kopiëren van gegevens.

Verantwoordelijke, verwerken, overeenkomst

Aangezien de gegevens van aanvragers persoonsgegevens zijn, is het van belang bij het verwerken van deze gegevens voortdurend rekening te houden met de wet- en regelgeving. Wij zijn namelijk verantwoordelijk voor het verwerken van deze gegevens. De wet noemt ons in dit geval de 'verwerkingsverantwoordelijke' voor de omgang met deze gegevens. Wanneer wij derde partijen inschakelen om namens ons deze gegevens te verwerken, bijvoorbeeld een partij die gegevens voor ons opslaat, cookies faciliteert of

gegevens analyseert, dan noemen we dergelijke partijen 'verwerkers'. Deze partijen verwerken dan in opdracht van ons persoonsgegevens.

Met verwerkers wordt altijd een verwerkersovereenkomst gesloten. Deze overeenkomst is wettelijk verplicht als persoonsgegevens verwerkt worden door een verwerker in opdracht van een verwerkingsverantwoordelijke. Hierin is opgenomen welke gegevens verstrekt worden en voor welke doeleinden de verwerker deze gegevens mag verwerken. Het is daarom ook van belang dat wanneer je gebruik wilt maken van de diensten van een derde partij, je altijd vooraf bij inkoop, bij de Privacy Officer of Coördinator IB&P controleert of de vereiste afspraken met deze partij zijn gemaakt.

Verwerken

Aangezien de gegevens van de aanvragers persoonsgegevens zijn, is het belangrijk om bij het verwerken van deze gegevens voortdurend rekening te houden met de belangen van de betrokkenen, maar ook de wettelijke verplichtingen van het Instituut.

Het mag voor een betrokkene geen verrassing zijn welke gegevens van hem gebruikt worden. Een betrokkene moet van te voren kunnen weten wat hij van ons kan verwachten. Op deze manier is het mogelijk een betrouwbare organisatie te blijven, en het vertrouwen in het schadeafhandelingsproces te vergroten.

Om als organisatie een goed overzicht te houden over de gegevens waarmee binnen het Instituut wordt gewerkt, zijn er een vijftal vragen opgesteld die over het gebruik van gegevens beantwoord moeten kunnen worden.

Aan de hand van deze vragen kan duidelijkheid worden verkregen hoe met de gegevens moet worden omgegaan en aan welke regels moet worden gehouden zodat het Instituut als organisatie voldoet aan de wet- en regelgeving. Het is daarom belangrijk dat je de volgende vijf vragen bij elke nieuw gebruik van de gegevens en informatiebron, kan beantwoorden:

1. Wat is de oorsprong van de gegevens waarmee gewerkt wordt?

Geef aan waar de gegevens vandaan komen. Zijn deze bijvoorbeeld door de betrokkene opgegeven bij een aanvraag, via een webformulier of via tracking cookies op de website?

2. Wat is de classificatie van deze gegevens (persoonsgegevens, etc.)?

Geef aan om wat voor gegevens het gaat. Gaat het bijvoorbeeld om NAW-gegevens, bankgegevens, zoekgedrag, medische gegevens, of bepaalde voorkeuren?

3. Waar worden deze gegevens verwerkt, en in welke systemen en/of omgeving/locatie?

Bijvoorbeeld: Bestanden staan in (het datacenter van) Atabix en worden verwerkt in Mira.

4. Wie heeft toegang tot deze gegevens?

Benoem alle personen of functies van de betrokken partijen die toegang tot deze gegevens hebben. In het geval van gegevens in de personeelsadministratie zouden dit bijvoorbeeld medewerkers van P&O kunnen zijn.

5. Hoe wordt met deze gegevens omgegaan? Denk hierbij aan onder andere: beveiliging, opslag, archivering, mutatie en vernietiging?

Geef aan welke beveiligingseisen men hanteert (bijvoorbeeld ISO norm 27001), hoe omgegaan wordt met archiveren en wanneer de gegevens worden vernietigd. Veelal is er een beveiligingsbeleid op te vragen.¹

Indien het verwerken van de gegevens een onderdeel van een project is, kun je ondersteuning binnen het project krijgen. Vaak kunnen de projectteams samen de vragen beantwoorden.

Indien je geen helder antwoord kunt geven op één van bovenstaande vijf vragen, of als dit antwoord onduidelijk dan wel onvolledig is, voldoen wij mogelijk niet onze wettelijke verplichtingen. Dit kan ertoe leiden dat de persoonsgegevens niet op de voorziene manier kunnen worden gebruikt. Als je twijfelt over de vraag of persoonsgegevens voor een bepaald doel gebruikt mogen worden, neem dan contact op met de Coördinator IB&P of de Privacy Officers. Het kan nodig zijn dat vóór het gebruik van de gegevens andere maatregelen genomen moeten worden, bijvoorbeeld het sluiten van een verwerkersovereenkomst of het uitvoeren van een Data Protection Impact Assessment (DPIA). Anderzijds is het mogelijk om een geaccepteerd risico te benoemen welke schriftelijk door het MT vastgelegd wordt. Dit geaccepteerde risico wordt door het MT vastgesteld op advies van de proceseigenaar en de Privacy Officers.

De toetsing van deze vragen moet ook periodiek op reeds bestaande verwerkingen uitgevoerd worden. Deze toetsing is een onderdeel van de jaarlijkse cyclus vanuit het security- en privacyplan, waarin de Privacy Officers langs alle afdelingen gaan. Door deze toetsing kunnen we inzicht en controle houden op de gegevens die worden verwerkt binnen het Instituut.

Als je twijfelt of bepaalde persoonsgegevens wel gebruikt mogen worden, wanneer je gegevens moet verstrekken aan derde partijen, of indien je vragen hebt over specifieke gegevens, neem dan direct contact op met de Privacy Officers of de Coördinator IB&P.

2.3 Soorten persoonsgegevens

Er worden verschillende persoonsgegevens in onze systemen verwerkt. Dit zijn bijvoorbeeld gegevens van medewerkers die door de P&O-afdeling worden ingevuld, of gegevens van aanvragers.

Voorbeelden van gegevens van aanvragers die in onze systemen worden verwerkt zijn:

- **Basisgegevens:**
 - NAW-gegevens;
 - telefoonnummer;
 - e-mailadres;
 - geslacht;
 - geboortedatum;
 - dossiernummer;
 - burgerservicenummer.
- **In een later stadium:**
 - schaderapporten;
 - correspondentie met IMG;
 - medische gegevens.

Bijzondere persoonsgegevens

Sommige persoonsgegevens kunnen daarnaast nog aangemerkt worden als 'bijzondere persoonsgegevens'. Bijzondere persoonsgegevens zijn gegevens die direct of indirect iets zeggen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap

¹ Ons interne beveiligingsbeleid is op te vragen bij de CISO.

van een vakvereniging. Het is mogelijk dat mensen aan ons bijzondere persoonsgegevens verstrekken bijvoorbeeld middels brieven, mails en/of telefoontjes. Het is van belang dat wij zorgvuldig omgaan met dit soort gegevens en dit beknopt vastleggen, maar alleen wanneer dit noodzakelijk is. Daarnaast moeten we deze gegevens goed beveiligen, niet delen met derden en mogen alleen de bevoegde medewerkers met deze gegevens werken.

Van onze medewerkers worden ook bijzondere persoonsgegevens verwerkt. Het is voor het Instituut toegestaan deze gegevens te verwerken indien dat noodzakelijk is voor de goede uitvoering van de arbeidsovereenkomst of bij re-integratie of begeleiding van een werknemer in verband met ziekte of arbeidsongeschiktheid. Dit is het geval als een medewerker bijvoorbeeld epilepsie heeft. Hiervan dienen wij op de hoogte te zijn, zodat wij op een juiste wijze kunnen handelen in een acute situatie. Het is echter niet toegestaan altijd bij een ziekmelding te noteren waarom iemand afwezig is, dit wordt daarom ook niet door de P&O-afdeling gedaan.

Register

Om alle verwerkingen allemaal inzichtelijk te krijgen en te houden, zijn wij verplicht een register bij te houden. Dit register bevat continu een up-to-date overzicht van alle soorten persoonsgegevens die wij verwerken. Dit register is te vinden op <https://www.avgregisterrijksoverheid.nl/>. Omdat wij verplicht zijn om deze registers up-to-date te houden, vragen wij je om eventuele wijzigingen zo spoedig mogelijk door te geven aan een van de Privacy Officers.

2.4 Doeleinden verwerken gegevens

Alle (persoons)gegevens worden door het Instituut voor specifieke doeleinden verwerkt. Gegevens mogen in principe alleen voor die doeleinden worden verwerkt, waarvoor ze zijn verzameld. Wij gebruiken de persoonsgegevens voor onze taak van algemeen belang, namelijk het afhandelen van schade veroorzaakt door mijnbouw in het Groningenveld of de gasopslag Norg. In sommige gevallen is de gegevensverwerking gebaseerd op het gerechtvaardigd belang, bijvoorbeeld bij cameratoezicht in de gebouwen, of toestemming, bijvoorbeeld voor de vermelding van je verjaardag op PLEK. Omdat we het vertrouwen van betrokkenen niet willen schenden vinden we het belangrijk dat gegevens niet worden gebruikt voor andere doeleinden waar de betrokkene niets van weet. Wil jij of het projectteam de gegevens voor een ander doel gebruiken, neem dan eerst contact op met het privacyteam. Mogelijk zitten er wettelijke beperkingen aan het gebruik van de gegevens of is er toestemming vereist van het MT.

Vanzelfsprekend worden gegevens van onze medewerkers verwerkt om de personeelsadministratie op een juiste manier uit te voeren. Gegevens van medewerkers mogen enkel door P&O gebruikt worden voor de taken die zij toegewezen hebben gekregen, of andere afdelingen indien zij ook concrete taken toegewezen hebben gekregen waarbij het verwerken van gegevens van medewerkers noodzakelijk is, zoals de OR. Gegevens van medewerkers worden verwerkt voor onder andere:

- het verwerken van de loonadministratie;
- het regelen van ziekte en verlof; en
- het regelen van in- en uitdiensttreding.

Kijk voor meer informatie over de gegevensverwerking van medewerkers in de interne privacyverklaring op PLEK. Daarnaast is de externe privacyverklaring te vinden op onze website. Twijfel je of gegevens van medewerkers voor een specifiek doel gebruikt mogen worden? Neem dan contact op met de Coördinator IB/AVG of Privacy Officer.