

met de aanvrager over zijn aanvraag. Het BSN wordt alleen verwerkt om burger te identificeren en om de rechthebbende van een kadastraal object vast te stellen. Het bankrekeningnummer wordt verwerkt om eventueel een vergoeding over te maken. De handtekening op de vaststellingsovereenkomst wordt verwerkt om een rechtsgeldige overeenkomst te sluiten met de aanvrager. De gegevens van de deskundigen worden alleen verwerkt om opnames in te plannen en om met de deskundigen te communiceren over de hen opgeleverde schaderapportages. Uit voorgaand blijkt dat alleen de noodzakelijke gegevens worden verwerkt voor het afhandelen van schade van aanvragers. Daarbij komt dat alleen de medewerkers toegang hebben tot deze dossiers die in het kader van hun werkzaamheden toegang tot deze dossiers moeten hebben. Dit geldt eveneens voor de deskundigen. Gevoelige gegevens, zoals uitingen over seksuele voorkeur of religie, worden daarnaast op foto's geblurd door de deskundigen. Daarmee zijn er voldoende waarborgen getroffen om de inbreuk op de persoonlijke levenssfeer te waarborgen.

Subsidiariteit

De regelingen Forfaitair worden op dezelfde wijze afgehandeld op technisch en administratief vlak als bij het fysieke schadeafhandelingstraject. Gedurende het opstellen van deze DPIA heeft het privacyteam geconstateerd dat op regeling breed niveau binnen het Instituut de volgende werkwijze wordt gehanteerd:

*"Tijdens het doen van een aanvraag levert de vertegenwoordiger het Instituut informatie over het kadastraal perceel aan.¹⁷ Als het Instituut in de aanvraag kan vaststellen dat iemand de rechtmatige eigenaar is (namelijk door het BSN aan het gekoppelde DigiD te vergelijken met de kadastrale informatie) dan kan het Instituut gelijk de informatie over het perceel tonen. Het Instituut toont dan ook de mede-eigenaren, zonder BSN maar met voor-/ en achternaam. Als iemand echter handmatig een perceel opvoert (bijvoorbeeld omdat er sprake is van een machtiging zonder DigiD) kan het Instituut de rechtmatige eigenaar niet vaststellen en toont deze geen informatie op voorhand. Het Instituut vraagt vervolgens om, naast de kadastrale informatie, ook de gegevens van de mede-eigenaren op te voeren door de voornaam, achternaam, en **BSN** aan te leveren".*

Het Instituut vraagt vertegenwoordigers/mede-eigenaren middels deze werkwijze om het uitwisselen van een gevoelig persoonsgegeven, namelijk een BSN. Deze werkwijze is om verschillende redenen onwenselijk en strookt bovendien niet met het subsidiariteitsbeginsel. Ten eerste is het BSN bedoeld om de overheid te laten communiceren met de burger, niet als ruilmiddel voor burgers onderling. Ten tweede stelt het Instituut hier niet mee vast of (mede)-eigenaar/volmachtgever daadwerkelijk aanspraak wil maken op een schadevergoeding. Tot slot kan dit leiden misbruik: de opvoerder zou zonder toestemming van de mede-eigenaar/volmachtgever gegevens kunnen gebruiken om zelf aanspraak te maken op schadevergoeding zonder dat de mede-eigenaar/ volmachtgever hierover wordt geïnformeerd.

Er bestaan daarnaast minder ingrijpende manieren om (mede)-eigenaren/volmachtgevers een aanvraag af te laten ronden waarbij zij worden geïdentificeerd als rechthebbenden:

¹⁷ Met vertegenwoordiger wordt de aanvrager of een gemachtigde bedoeld.

- Een tekensessie: De volmachtgever/mede-eigenaar krijgt per e-mail of via 'Mijn Overheid'/'Berichtenbox' een tekenverzoek/ DigiD-inlogverzoek. Via dit verzoek vult de persoon zijn gegevens in; en
- het Instituut haalt de (BSN-)gegevens uit het kadaster/BRP en neemt contact op met de vertegenwoordiger om de opgevraagde gegevens te bevestigen. In dit geval vraagt het Instituut aan de gemachtigde/mede-eigenaar om de laatste 3 cijfers te bevestigen van het BSN. Hierdoor hoeft de aanvrager/vertegenwoordiger alleen maar de laatste drie cijfers van BSN aan zijn mede-eigenaren te vragen en hebben we wel de juistheid van zowel het nummer, als de aanvraag, als de identiteit van de mede-eigenaar geverifieerd;
- In het verleden is gebleken dat de combinatie voornaam/achternaam en geboortedatum niet robuust genoeg is als zoekingang. Het komt dan alsnog voor dat er dubbelingen optreden waar uiteindelijk de verkeerde persoon wordt geraadpleegd en wordt opgevoerd. Als extra waarborg kan dan ook nog zijn om de postcode en huisnummer toe te voegen. Zo verwerken we wel wat meer gegevens, maar geen gevoeligere gegevens van betrokkenen.

Gelet op de risico's en de andere wijzen voor het realiseren van het identificeren van een rechthebbende bij een kadastraal object, kan deze verwerking **niet** als noodzakelijk worden beschouwd. Daarmee is het identificeren van rechthebbenden op deze wijze niet in lijn met de AVG. Het Instituut zal derhalve een andere wijze moeten implementeren voor het identificeren van een rechthebbende. Zo is reeds door de privacy officers en de Functionaris Gegevensbescherming geadviseerd alvorens de onderhavige DPIA is afgerond.

Het Instituut heeft er voor gekozen eerst de AVV-regeling te realiseren op 1 november 2024. Daarnaast dient het Instituut conform een audit van Logius zijn beveiliging op orde te krijgen. Voorgenoemde onderwerpen vergen veel capaciteit en tijd van de IT-dienst van het Instituut. Het opleveren van de AVV-regeling op 1 november 2024 is een belofte die het Instituut dient waar te maken aan het Tweede Kamer en de Groningse bevolking naar aanleiding van het rapport 'Groningers boven Gas'. Tevens dient het Instituut voor 1 mei 2025 de beveiliging van het inlogportaal op orde te krijgen, dit is de uiterlijke deadline voor het implementeren van de maatregelen van de audit van Logius. Om die reden heeft managementteam/ directieteam van het Instituut op 11 september 2024 ervoor gekozen om dit risico tijdelijk te accepteren.¹⁸

Voor de overige gegevens die nodig zijn voor de afhandeling van forfaitaire aanvragen zijn geen minder ingrijpende middelen mogelijk. Deze worden in de meeste gevallen uitgevraagd bij de betrokkenen zelf, en zijn ook allen nodig voor de afhandeling van de aanvragen.

¹⁸ Risico acceptatie 'Opvoeren BSN (mede)-eigenaar', getekend op 11 september 2024 .

15. Rechten van 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.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht op rectificatie en aanvulling	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht op vergetelheid	Procedure voor de rechten van betrokkenen van het Instituut	Op grond van de archiefwet is het Instituut verplicht de gegevens uit schadedossiers blijvend te bewaren
Recht op beperking van de verwerking	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht op dataportabiliteit	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht om bezwaar te maken	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.
Recht op duidelijke informatie	Procedure voor de rechten van betrokkenen van het Instituut	n.v.t.

Op grond van de AVG heeft de betrokkene een aantal rechten. Daarom stelt het IMG de betrokkene in staat om zijn of haar privacyrechten uit te oefenen.

Een betrokkene kan zijn of haar rechten uitoefenen door een AVG-verzoek in te dienen (telefonisch of digitaal (e-mail of DigiD)).

Ook kan de betrokkene zelf via de 'Mijn Dossier'-omgeving informatie verstrekken/wijzigingen doorgeven wat betreft diens persoonlijke situatie. Om gehoor te kunnen geven aan de rechten van betrokkenen, zijn de systemen, processen, en interne organisatie van IMG op deze rechten ingericht

Op de website van het Instituut staat de privacyverklaring, waarin uitgelegd staat dat de betrokkene de mogelijkheid heeft zijn of haar privacyrechten uit te oefenen.

Daarnaast zijn er zaakbegeleiders die regelmatig contact hebben met betrokkenen (aanvragers). Zij kunnen de betrokkenen ook informeren over de privacyrechten.

Via een uitleg of verklaring op de website wordt voldaan aan de informatieplicht. Het Instituut heeft op haar website en in de privacyverklaring zo veel mogelijk informatie opgenomen over de gegevensverwerking. Daarnaast zal het Instituut ook op het aanvraagformulier verwijzen naar de privacyverklaring.

Zoals hierboven bij de bewaartermijnen uitgewerkt is, moet het Instituut de gegevens die zien op de primaire taak van het Instituut (het afhandelen van schade) blijvend bewaren. Hierdoor kan er in de meeste gevallen niet worden voldaan aan een verwijderingsverzoek wanneer betrokkenen deze indienen. Forfaitaire schadevergoeding is een primair proces, waardoor de gegevens die hiervoor in een dossier worden verwerkt blijvend bewaard moeten worden bij het Nationaal Archief (met een openbaarheidsbeperking). Wanneer aanvragers bijvoorbeeld extra informatie per mail verzenden, moet bij een verwijderingsverzoek worden beoordeeld of deze informatie wel verwijderd kan worden.

Beschrijving en beoordeling risico's voor de betrokkenen

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

16. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij 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;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus **laag**, **'gemiddeld'** en **hoog**. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.

		Kans		
		laag	midden	hoog
Impact	hoog	hoog	hoog	hoog
	midden		midden	hoog
	laag			

*De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.

Voeg aanvullende informatie in het tekstveld toe.

Beschrijving risico	Kans	Impact	Risico-inschatting
Risico het Instituut: Door het opvoeren van BSN's door anderen personen kunnen er per abuis verkeerde BSN's worden verwerkt in de systemen van het Instituut. Dit is in strijd met juistheidbeginsel .	Hoog: door het handmatig laten opvoeren van BSN's is de kans op een menselijke fout aanzienlijk, waardoor het Instituut onjuiste gegevens verwerkt.	Laag: het onjuist verwerken van BSN's is in strijd met de AVG, maar leidt niet tot impactvolle risico's op het gebied van juistheid. Voor het uitvoeren van de forfaitaire regelingen wordt er immers altijd een	Laag.

Beschrijving risico	Kans	Impact	Risico-inschatting
		eigendomscontrole uitgevoerd door het Instituut. Bij ontdekking van de invoering van een onjuist BSN, zal het Instituut maatregelen nemen om dit te corrigeren.	
Risico betrokkenen: Gegevens die op Atabix worden verwerkt kunnen op servers in Amerika worden opgeslagen	Laag: op basis van de afspraken moeten gegevens in de EER worden opgeslagen	Laag: Atabix valt onder AWS, welke onder het Data Privacy Framework vallen.	Laag.
Risico betrokkenen: Door het opvoeren van BSN's door anderen personen kunnen er per abuis verkeerde BSN's worden verwerkt in de systemen van het Instituut, waardoor de verkeerde persoon wordt gekoppeld aan een dossier. Deze koppeling is volgens de wet al een datalek . Daarnaast zou er tevens naar de verkeerde persoon documentatie kunnen worden verzonden hetgeen ook een datalek betreft.	Hoog: de kans is weer hoog doordat een aanvrager zelf de BSN's dient op te voeren, van de aanvrager zelf en de mede-eigenaar.	Midden: datalekken kunnen leiden tot identiteitsfraude en financiële schade voor betrokkenen. Nu wij niet met zekerheid kunnen vaststellen of de (mede-) eigenaar ook daadwerkelijk de aanvraag bij deze werkwijze wordt de risico-inschatting op hoog gezet.	Hoog.
Risico het Instituut: Door het opvoeren van BSN's door andere personen handelt het Instituut in strijd met rechtmatigheidsbeginsel. Dit zou bij ontdekking van deze handelswijze door de Autoriteit Persoonsgegevens (AP) ertoe kunnen leiden dat de AP beveelt de verwerkingen te stoppen . Dat zou betekenen dat het Instituut	Hoog: Zie toelichting bij het subsidiariteitsbeginsel. Deze werkwijze is onrechtmatig. Daarnaast is het Instituut onlangs slecht in het nieuws geweest met betrekking tot een audit en zijn privacybeleid. ¹⁹ Bovendien hebben we onlangs een brief van de AP gehad met	Hoog: De impact wordt hoog ingeschat, omdat dit kan leiden tot reputatieschade. Het vertrouwen van de burger in het Instituut is al laag. Daarbij komt dat indien de AP ons beveelt om de verwerkingen dit leidt tot nadelige gevolgen voor de burger. Wij	Hoog.

¹⁹ OOG TV 2024, *Vooral verbeteringen op papier in het privacybeleid IMG, praktijk laat nog te wensen over* gepubliceerd op 16 september 2024, laatst geraadpleegd op 20 september 2024, zie link: [Vooral verbeteringen op papier in privacybeleid IMG, praktijk laat nog te wensen over | OOG Groningen \(oogtv.nl\)](#).

Beschrijving risico	Kans	Impact	Risico- inschatting
geen schade meer kan afhandelen tot dat deze verwerkingen conform de AVG worden toegepast. Tevens kan het leiden tot boetes en berispingen en daarnaast kan het tot reputatieschade leiden.	betrekking tot een klacht van betrokkene. De kans dat de AP op termijn langs komt wordt daarom hoog ingeschat en als zij deze handelswijze ontdekt bestaat de kans ook dat zij ons een boete geeft of beveelt om bepaalde verwerkingen te stoppen.	zouden immers ons bedrijfsvoering tijdelijk moeten stoppen. Daarbij komt dat wij voorrang geven aan implementaties van andere maatregelen, hetgeen deze onrechtmatigheid voor op zijn minst 10 maanden laat voortduren. Daarbij wordt de kans op ontdekking van een de AP vergroot.	
Risico het Instituut: De selectielijst van EZK is nog niet definitief vastgesteld bij het Nationaal Archief. Hierdoor kunnen er nog wijzigingen in gemaakt worden, terwijl we deze selectielijst op dit moment als uitgangspunt gebruiken.	Laag: we mogen deze lijst ook als uitgangspunt gebruiken, ondanks dat deze nog niet is vastgesteld. De lijst is bovendien zorgvuldig opgesteld waardoor wijzigingen waarschijnlijk niet nodig zullen zijn.	Laag: grootste gevolg is het verwijderen van gegevens die niet verwijderd hadden mogen worden. Gezien het stempel "blijvend bewaren" is de mogelijkheid dat dit zich voordoet minimaal.	Laag.

Maatregelen en restrisico's

In onderdeel D wordt gezien 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.

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.

Geef tot slot een conclusie over de restryco's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Gebruik voor de inschattingen van de risico's de niveaus **laag**, 'gemiddeld' en **hoog**. Gebruikmaken van de bijbehorende kleuren is aan te raden.

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Door het opvoeren van BSN's door anderen personen kunnen er per abuis verkeerde BSN's worden verwerkt in de systemen van het Instituut. Dit is in strijd met juistheidbeginsel .	Er wordt gewerkt aan een andere werkwijze die dit risico opheft. Deze is vooralsnog onbekend en kan derhalve niet worden ingevuld.	Laag	Projectteam, afhankelijk van prioritering maatregel door MT
Gegevens kunnen door Atabix in Amerika opgeslagen worden	Afspraken in de (verwerkingsovereenkomst gemaakt)	laag	Projectteam in samenspraak met privacy officer
Door het opvoeren van BSN's door anderen personen kunnen er per abuis verkeerde BSN's worden verwerkt in de systemen van het Instituut, waardoor de verkeerde persoon wordt gekoppeld aan een dossier. Alleen deze koppeling is volgens de wet al een datalek . Daarnaast zou er tevens naar de verkeerde persoon documentatie kunnen worden verzonden hetgeen ook een datalek betreft.	Er wordt gewerkt aan een andere werkwijze die dit risico opheft. Deze is vooralsnog onbekend en kan derhalve niet worden ingevuld.	Hoog	Projectteam, afhankelijk van prioritering maatregel door MT
Door het opvoeren van BSN's door andere personen handelt het Instituut in strijd met	Er wordt gewerkt aan een andere werkwijze die dit risico opheft. Deze is vooralsnog onbekend en	Hoog	Projectteam, afhankelijk van prioritering

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
rechtmatigheidsbeginsel. Dit zou bij ontdekking van deze handelswijze door de Autoriteit Persoonsgegevens (AP) ertoe kunnen leiden dat de AP beveelt de verwerkingen te stoppen . Dat zou betekenen dat het Instituut geen schade meer kan afhandelen tot dat deze verwerkingen conform de AVG worden toegepast. Tevens kan het leiden tot boetes en berispingen en daarnaast kan het tot reputatieschade leiden.	kan derhalve niet worden ingevuld.		maatregel door MT
De selectielijst van EZK is nog niet definitief vastgesteld bij het Nationaal Archief. Hierdoor kunnen er nog wijzigingen in gemaakt worden, terwijl we deze selectielijst op dit moment als uitgangspunt gebruiken.	De lijst wordt in Q4 van 2024 vastgesteld.	Laag	DIV.

Ondertekening

Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	5.1.2e
Directie/afdeling verantwoordelijke(n)	BJZ&S
Functie verantwoordelijke(n)	Afdelingsmanager
Datum ondertekening	24/10/'24
Handtekening	5.1.2e

Naam verantwoordelijke(n)	5.1.2e
Directie/afdeling verantwoordelijke(n)	IV
Functie verantwoordelijke(n)	Afdelingsmanager
Datum ondertekening	5/11/2024
Handtekening	5.1.2e

Naam: Herziende DPIA logging en monitoring.

Advies functionaris voor gegevensbescherming: 17-01-2025

Naam FG: 5.1.2e

Privacy officer: 5.1.2e en 5.1.2e

Versie: 1

Status: Definitief

Revisie:

Versie	Datum	Toelichting
Versie 0.1	12-12-2024	Concept
Versie 1	22-01-2025	Definitief

Inhoudsopgave

Advies FG 3

Managementsamenvatting 6

Beschrijving kenmerken gegevensverwerkingen 7

- 1. Voorstel 8**
- 2. Persoonsgegevens 9**
- 3. Gegevensverwerkingen 9**
- 4. Technieken en methoden van de gegevensverwerkingen 10**
- 5. Verwerkingsdoeleinden 11**
- 6. Betrokken partijen 11**
- 7. Belangen bij de gegevensverwerkingen 12**
- 8. Verwerkingslocaties 15**
- 9. Juridisch en beleidsmatig kader 15**
- 10. Bewaartermijnen 16**

Beoordeling rechtmatigheid gegevensverwerkingen 17

- 11. Rechtsgrond 17**
- 12. Bijzondere persoonsgegevens 20**
- 13. Doelbinding 20**
- 14. Noodzaak en evenredigheid 22**

Beschrijving en beoordeling risico's voor de betrokkenen 25

- 15. Risico's voor betrokkenen 25**
- 16. Maatregelen 27**

Ondertekening 28

Advies FG

Aanleiding

Het Instituut Mijnbouwschade Groningen (hierna: 'het Instituut') is bevoegd om te beslissen over aanvragen voor vergoeding van fysieke schade aan gebouwen en werken, maar kan ook andere vormen van schade behandelen. Andere vormen van schade zijn bijvoorbeeld waardedaling en immateriële schade. Immateriële schade ('IMS') betreft schade die niet financieel van aard is, zoals pijn, geestelijk leed, verdriet of het verlies van levensvreugde. De vergoeding hiervoor, ook wel 'smartengeld' genoemd, heeft als doel het leed van de betrokkene te verzachten en hem of haar een vorm van genoegdoening te bieden.

Het toekennen van deze vergoeding gaat inherent gepaard met het verwerken van gezondheidsgegevens. De medewerkers van de afdeling juridische zaken ('JZ-medewerkers') binnen het team Waardedaling en Immaterieel hebben toegang tot gezondheidsgegevens van IMS-aanvragers, waaronder:

- gezondheidsgegevens door de aanvrager zelf ingegeven;
- gezondheidsgegevens in bewijsstukken die de aanvragen opstuurt;
- de persoonlijke impact analyse (PIA) die de aanvrager invult;
- de PIA scores binnen het huishouden.

Deze toegang, waarbij het specifiek gaat om de inzage in de vragenlijsten en het raadplegen van de gezondheidsgegevens door medewerkers, wordt gelogd. Deze logbestanden worden op de beveiligde applicatie MIRA opgeslagen en kunnen niet door de medewerkers worden aangepast of verwijderd. Het loggen van de gegevens gebeurt in overeenstemming met het Logging- en Monitoringsbeleid. Dit voorkomt willekeur.

Omdat het (indirect) gaat om het (verder) verwerken van bijzondere persoonsgegevens van een grote groep kwetsbare betrokkenen, namelijk gezondheidsgegevens van aanvragers, is een (verplichte) DPIA uitgevoerd voor deze verwerking. Deze DPIA en het bijbehorende advies zal als addendum worden toegevoegd aan de DPIA IMS.

Doel van het gewenste proces

Het monitoren en loggen van medewerkers op hun activiteiten omtrent het inzien van vragenlijsten heeft voor het Instituut primair als doel te helpen bij het maken van een belangenafweging tussen het beveiligen van de (persoons)gegevens en het recht op privacy van de medewerker. Het Instituut wil voldoende beveiliging waarborgen van de bijzondere persoonsgegevens van aanvragers en zij wil de vertrouwelijkheid en integriteit van gevoelige informatie garanderen.

Het loggen heeft daarnaast als doel dat aantoonbaar kan worden gemaakt dat een medewerker integer handelt. Het draagt daarmee direct bij aan het voorkomen van onrechtmatige toegang binnen de systemen van het Instituut. Het monitoren van logs helpt ook bij het identificeren van trends die wijzen op structurele beveiligingsproblemen.

Voordelen

Ten eerste biedt het voorgenomen proces van het loggen van medewerkers een aantal voordelen voor de betrokkenen. Deze voordelen worden hieronder kort besproken.

- 1) Het loggen van medewerkers kan medewerkers helpen om aan te kunnen tonen dat zij integer hebben gehandeld, bijvoorbeeld wanneer er een beveiligingsincident heeft plaatsgevonden.
- 2) Logging en monitoring vormen de basis van effectief databasebeheer en -beveiliging.
- 3) Logging en monitoring draagt bij aan het vertrouwen dat aanvragers hebben in het Instituut met betrekking tot hun privacy. Door de logging kan worden aangetoond dat enkel noodzakelijke toegang tot de persoonsgegevens plaatsvindt.

Aandachtspunten/risico's

Het monitoren en loggen van de handelingen van de medewerkers brengt een aantal risico's met zich mee. Met name gaat het hier over het informeren van de medewerkers over het feit dat hun werkzaamheden worden vastgelegd.

De FG onderschrijft de in de DPIA geconstateerde risico's. Hieronder worden die risico's nog kort toegelicht.

- 1) De huidige interne privacyverklaring voor medewerkers is op dit moment niet makkelijk toegankelijk/vindbaar. Hij staat wel op de intranetwebsite van het Instituut, maar er ontbreekt een gemakkelijk toegankelijk link. Het is van belang dat medewerkers de privacyverklaring makkelijk kunnen vinden en raadplegen omdat hierin informatie staat over hoe hun persoonsgegevens worden verwerkt, voor welke doeleinden, en hoe zij gebruik kunnen maken van hun rechten. Er kan bijvoorbeeld een opvallende knop worden opgenomen op de intranetwebsite die direct linkt naar de interne privacyverklaring.
- 2) Er ontbreekt op dit moment een sanctiebeleid voor medewerkers die oneigenlijk gebruik maken van hun inzagerechten. Zonder een dergelijk beleid zijn er geen duidelijke gevolgen voor medewerkers op het moment dat zij de werkinstructies niet volgen, waardoor ze minder worden ontmoedigd om hun toegang ongeoorloofd te gebruiken. Het is daarom van belang dat er een sanctiebeleid wordt opgesteld en dat deze ook met de medewerkers wordt gedeeld.

Als extra aanvulling is onderstaande punt van belang:

- 3) Uit de DPIA blijkt niet geheel duidelijk onder welke voorwaarden de logbestanden worden ingezien, behalve de maandelijkse controle door de Interne Controller. Mogelijk wordt in het Logging- en monitoringsbeleid nader toelichting gegeven over de 'triggers' waardoor inzage in de logbestanden mogelijk is. Het advies is om dit te controleren.

Omdat deze DPIA onderdeel zal worden van de DPIA IMS, wordt wellicht ten overvloede nog genoemd dat de risico's die uit die DPIA zijn gebleken, ook volgens de geplande maatregelen gemitigeerd dienen te worden.

Overige aandachtspunten

- 1) Onder het kopje 'Maatregelen en risico's' wordt gesproken over 'onderdeel C & D'. Deze onderdelen zijn niet terug te vinden in de DPIA. Het advies is om te verduidelijken welke paragraaf wordt bedoeld.

Conclusie

Het Instituut Mijnbouwschade Groningen (IMG) behandelt aanvragen voor vergoeding van immateriële schade, waaronder gezondheidsgegevens van aanvragers. De verwerking hiervan vereist een hoge mate van beveiliging. Het monitoren en loggen van medewerkers is cruciaal om de vertrouwelijkheid, integriteit, en veiligheid van deze gegevens te waarborgen en om integer handelen aan te tonen.

Ondanks de voordelen, zoals het vergroten van vertrouwen bij aanvragers en effectief databeheer, zijn er aandachtspunten. Deze hebben te maken met het feit dat de interne privacyverklaring niet makkelijk toegankelijk is voor medewerkers en dat het sanctiebeleid bij misbruik van inzagerechten ontbreekt.

Advies

Gezien de grote voordelen die het loggen en monitoren van de gegevens van de medewerkers met zich meebrengen, geef ik **onder voorbehoud een positief advies** op de voorgenoemde verwerking. Het is echter wel van belang dat de geconstateerde aandachtspunten tijdig geïmplementeerd worden.

Managementsamenvatting

De DPIA is uitgevoerd met als doel de rechten van zowel medewerkers als aanvragers te waarborgen bij het registreren van inzage in immateriële schadedossiers. Het proces was gericht op het identificeren en verminderen van risico's die voortvloeien uit de verwerking van persoonsgegevens binnen dit systeem. In dit kader zijn twee maatregelen aanbevolen:

- **Sanctiebeleid:** Om misbruik van inzagerechten door medewerkers te voorkomen, wordt de implementatie van een duidelijk sanctiebeleid voorgesteld.
- **Toegankelijkheid privacyverklaring:** Het wordt aanbevolen om de privacyverklaring voor medewerkers beter toegankelijk te maken door deze via een knop op het intranet beschikbaar te stellen, zodat medewerkers beter geïnformeerd zijn over hun rechten.

Na de implementatie van deze maatregelen worden alle geïdentificeerde risico's als laag beoordeeld.

Beschrijving kenmerken gegevensverwerkingen

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

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de DPIA is gebaseerd op wat in dit onderdeel is beschreven.

1. Voorstel

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

Het Instituut Mijnbouwschade Groningen (hierna: 'het Instituut') is niet alleen bevoegd om te beslissen over aanvragen voor vergoeding van fysieke schade aan gebouwen en werken, maar kan ook andere vormen van schade behandelen. Onder andere vormen van schade vallen bijvoorbeeld waardedaling en immateriële schade.

Immateriële schade betreft schade die niet financieel van aard is, maar op andere manieren wordt ervaren, zoals pijn, geestelijk leed, verdriet of het verlies van levensvreugde. De vergoeding hiervoor, ook wel 'smartengeld' genoemd, heeft als doel het leed van de betrokkene te verzachten en hem of haar een vorm van genoegdoening te bieden. Hoewel de term 'smartengeld' soms doet denken aan 'Amerikaanse toestanden', gaat het in Nederland om een doorgaans bescheiden vergoeding, die bovendien alleen in specifieke gevallen wordt toegekend.

Deze Data Protection Impact Assessment (DPIA) richt zich op de logging- en monitoring van de juridische zaken medewerkers (JZ-medewerkers) van het team: Waardedaling en Immaterieel, die toegang hebben tot gezondheidsgegevens van IMS aanvragers waaronder:

- gezondheidsgegevens door de aanvrager zelf ingegeven;
- gezondheidsgegevens in bewijsstukken die de aanvragen opstuurt;
- de persoonlijke impact analyse (PIA) die de aanvrager invult;
- de PIA scores binnen het huishouden.

De JZ-medewerkers hebben ook toegang tot andere gegevens van de IMS aanvragers. Dit is geen onderdeel van deze DPIA.

De verwerking van persoonsgegevens met betrekking tot logging- en monitoring is opgenomen in het verwerkingsregister van het Instituut.

Deze DPIA zal als addendum worden toegevoegd aan de DPIA Immateriële Schade (hierna: 'IMS').¹ Het betreft namelijk een proces die plaatsvindt bij de regeling IMS. Omdat op dit proces een aparte DPIA is uitgevoerd en onderhevig is aan herziening wordt voor nu gekozen om dit proces apart te herzien, maar in de toekomst zal de herziene toets van dit proces plaatsvinden bij de herziening van de DPIA IMS.

¹ 5.1.2e 2023, *Herziene DPIA Immateriële Schade*, herzien en getekend op 11 december 2023.

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.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatienummer)	Bron
Medewerkers	Gewoon	Naam (voor- en achternaam)	Gewoon	Logging IMS dossiers
Medewerkers	Gewoon	E-mailadres	Gewoon	Logging IMS dossiers
Medewerkers	Gewoon	Functie	Gewoon	Logging IMS dossiers
Medewerkers	Gewoon	Tijdstip	Gewoon	Logging IMS dossiers
Medewerkers	Gewoon	(mogelijk)IP-adres (tijdens het thuiswerken)	Gewoon	Logging IMS dossiers

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.

Gegevensverwerking	Categorieën persoonsgegevens
Logging	NAW, contact, functie, tijdstip en IT. (medewerker)
monitoring	NAW, contact, functie, tijdstip en IT. (medewerker)

Bij elke inzage in een PIA is het verplicht dat de medewerker een reden opgeeft voor het raadplegen van de gegevens. Deze reden wordt samen met de naam van de medewerker, de datum en het tijdstip van inzage automatisch geregistreerd in een logbestand.

Naast de inzage in vragenlijsten die door aanvragers zijn ingevuld, wordt ook de raadpleging van andere gezondheidsgegevens door medewerkers gelogd waaronder:

- gezondheidsgegevens door de aanvrager zelf ingegeven;
- gezondheidsgegevens in bewijsstukken die de aanvragen opstuurt;
- de persoonlijke impact analyse (PIA) die de aanvrager invult;
- de PIA scores binnen het huishouden.

Het logbestand wordt op de beveiligde applicatie MIRA opgeslagen en kan niet door de medewerkers zelf worden aangepast of verwijderd. De logging registreert alle toegangspogingen, inclusief zowel succesvolle als mislukte pogingen. Dit maakt het mogelijk om ongeautoriseerde toegangspogingen tijdig te signaleren.

De afdelingsmanager van IMS verstrekt autorisaties uitsluitend aan JZ-medewerkers die deze daadwerkelijk nodig hebben voor hun werkzaamheden. Dit zorgt ervoor dat gevoelige informatie goed beschermd blijft. De logging van JZ-medewerkers dient 1 keer per maand beoordeeld te worden door de Teammanager Functioneel Beheer. Rapportage van deze controle dient naar de Security Officer gestuurd te worden met een analyse of er discrepanties zijn geweest in toegangsrechten. De Security Officer handelt de discrepantie af als een beveiligingsgebeurtenis.

Het monitoringsproces waarborgt dat alleen noodzakelijke toegang tot persoonsgegevens plaatsvindt. Bovendien biedt het inzicht in wie, wanneer en waarom toegang heeft gehad, waardoor misbruik kan worden voorkomen. Dit proces bevordert de integriteit van de gegevens.

4. Technieken en methoden van de gegevensverwerkingen

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

Bij de behandeling van de vragenlijsten van aanvragers binnen de regeling immateriële schade worden JZ-medewerkers gelogd en gemonitord. Hierbij wordt geen gebruik gemaakt van (semi-)geautomatiseerde besluitvorming, profilering of big-data verwerking.

Op zaakniveau (dossierniveau) bij MIRA (waaronder regeling IMS) wordt gelogd. Daarbij wordt vastgelegd de naam van de medewerker, opgaaf van reden voor inzage en de datum en het tijdstip van inzage (auditlogging). Zie hiervoor ook het Logging- en Monitoringsbeleid.²

² 5.1.2e en 5.1.2e 2024, *Logging- en Monitoringsbeleid*, gepubliceerd op 6 november 2024.

Bij het loggen en monitoren van medewerkers die dossiers met bijzondere persoonsgegevens opvragen in MIRA, worden uitsluitend gegevens vastgelegd die nodig zijn om de toegang en het gebruik van deze dossiers te kunnen controleren. Het loggen omvat de registratie van de gebruikersidentiteit (gebruikers-ID), het tijdstip van toegang (tijdstempel), het specifieke dossier dat is opgevraagd (dossier-ID), en de acties die binnen het dossier zijn uitgevoerd, zoals bekijken of bewerken. Deze gegevens worden op een veilige en centraal beheerde locatie opgeslagen en zijn uitsluitend toegankelijk voor bevoegde personen.

5. Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.
Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
Logging	Controleren van medewerkers op hun activiteiten omtrent het inzien van de vragenlijsten.	De afspraken uit de arbeidsovereenkomst nakomen en uitvoeren.
Monitoring	Controleren van medewerkers op hun activiteiten omtrent het inzien van de vragenlijsten.	De afspraken uit de arbeidsovereenkomst nakomen en uitvoeren.

Bij logging- en monitoring worden de (persoons)gegevens van JZ-medewerkers verwerkt met als doel de medewerkers te controleren op hun activiteiten omtrent het inzien van de (gezondheids)gegevens en vragenlijsten (Persoonlijke Impact Analyse - PIA) van aanvragers.

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. Voeg aanvullende informatie toe in het tekstveld.

Naam partij	Rol partij	Functies/afdelingen	Persoonsgegevens
IMG	Verwerkingsverantwoordelijke	• Functionarissen auditlogging; • Functioneel beheerder; • Interne controller/ auditor; • Behandelend JZ-medewerker.	NAW, contact, functie, tijdstip en IT. (medewerker)
DICTU	Verwerker	n.v.t.	NAW, contact, functie, tijdstip en IT. (medewerker)
Auditdienst Rijk	Ontvanger	n.v.t.	NAW, contact, functie, tijdstip en IT. (medewerker)

Deze paragraaf gaat in op de betrokken partijen bij de voorgenomen gegevensverwerkingen. De volgende partijen zijn hierbij betrokken:

Verwerkingsverantwoordelijke: het Instituut. Het Instituut is een zelfstandig bestuursorgaan, en valt dus niet onder de directe bevoegdheid van één van de ministeries. Het bestuur van het Instituut stelt dus zelf het doel, de middelen, en de verwerkingen vast die hij in het kader van het uitoefenen van zijn bevoegdheden uitvoert.

Medewerkers van het Instituut hebben toegang tot de persoonsgegevens en het beeldmateriaal dat aanvragers aanleveren bij het doen van een aanvraag tot schadevergoeding.

Verwerker(s)

- DICTU (ICT).

Verstrekker(s) van persoonsgegevens

- Behandelend JZ-medewerker van het Instituut.

Ontvangers van persoonsgegevens

- Auditdienst Rijk.

Functionarissen

- Functionarissen auditlogging van het Instituut;
- Functioneel beheerder van het Instituut;
- Interne controller/ auditor van het Instituut.

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.

Betrokken Partij	Belangen
Het Instituut	Zie hieronder.
JZ-medewerkers	Zie hieronder.
ADR	Zie hieronder.
DICTU	Zie hieronder.
Aanvragers	Zie hieronder.

Het Instituut

Organisatorisch/operationeel belang, voldoen aan wettelijke taak: conform artikel 2 lid 3 TwG heeft het Instituut de wettelijke taak om schade af te handelen. Onder het afhandelen van schade valt ook de behandeling van aanvragen van de IMS regeling.³ Om aan deze taak te voldoen, moet het Instituut persoonsgegevens verwerken.

Het logging- en monitoringbeleid heeft als doel te helpen bij het maken van een belangenafweging tussen het beveiligen van de (persoons)gegevens en het recht op privacy van de medewerker.

Behandelend JZ-medewerkers van het Instituut

Voor medewerkers betekent het loggen een beperking in hun privacy. Toch is het loggen ook in hun belang, omdat het bijdraagt aan integer handelen dat ook aantoonbaar is. Belangrijk is dat het inperken van hun privacy niet zomaar mag. Het loggen mag alleen als wordt voldaan aan de beleidskaders hiervoor (het Logging- en Monitoringbeleid). Dat voorkomt willekeur en geeft duidelijkheid aan de medewerkers.

Auditdienst Rijk (hierna: ADR)

Organisatorisch/operationeel belang: wanneer de ADR de opdracht krijgt om een audit uit te voeren bij het Instituut, dienen zij uit hoofde van die opdracht toegang te hebben tot bepaalde (persoons)gegevens van het Instituut, waaronder gegevens die in het kader van de IMS regeling verzameld zijn.

DICTU (Dienst ICT Uitvoering)

Organisatorisch/operationeel belang: DICTU is vanuit het Rijk belast met het faciliteren van ICT aan overheidsorganen. Vanuit die hoedanigheid hebben zij een belang bij de verwerking van persoonsgegevens door het Instituut.

Aanvragers (eigenaren en gemachtigden – zijnde natuurlijke personen, bedrijven en woningcorporaties)

Persoonlijk/privacy belang: de aanvragers hebben allereerst een belang bij een nauwkeurige beoordeling van hun aanvraag tot compensatie als gevolg van de waardedaling van hun woning en/of bedrijfspand. Daarnaast hebben de aanvragers een belang bij eerbiediging van hun privacy, omdat er in het proces (gevoelige) persoonsgegevens van hen kunnen worden verwerkt.

³ Zie Rb. Noord-Nederland, 1 november 2021, ECLI:NL:GHARL:2018:618.

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. Voeg aanvullende informatie toe in het tekstveld.

Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.

Gegevensverwerkingen	Verwerkingslocaties	Doorgiftemechanisme	Maatregelen
Logging	Nederland	n.v.t.	n.v.t.
Monitoring	Nederland	n.v.t.	n.v.t.

Alle verwerkingen vinden in Nederland plaats.

9. Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn⁴ hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Logging	Zie hieronder.	Zie hieronder.
Monitoring	Zie hieronder.	Zie hieronder.

Het Instituut heeft tot taak om schade af te handelen die is ontstaan door beweging van de bodem als gevolg van de aanleg of exploitatie van een mijnbouwwerk ten behoeve van het winnen van gas uit het Groningenveld of als gevolg van de gasopslag Norg. Het Instituut is bij de uitvoering van zijn taak onder meer gebonden aan de Tijdelijke wet Groningen (TwG). Hieruit volgt dat het Instituut zijn taak op onafhankelijke en rechtvaardige wijze dient uit te voeren. Hierbij dient het Instituut toepassing te geven aan het civiele aansprakelijkheids- en schadevergoedingsrecht en het bestuurs(proces)recht. Binnen deze kaders geeft het Instituut invulling aan zijn taak.

Logging- en Monitoringbeleid: logging en monitoring vormen de basis van effectief databeheer en -beveiliging. Logging houdt in dat alle activiteiten die betrekking hebben op de gegevens en de systemen van de organisatie worden vastgelegd. Monitoring aan de andere kant, omvat het continue toezicht op deze logs om afwijkingen, aanvallen of inbreuken op de beveiliging snel te identificeren.

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

Logging- en Monitoringbeleid en WOR: het Instituut behoeft de instemming van de OR op grond van artikel 27, eerste lid, aanhef en onder k en l, Wet op de Ondernemingsraden.

Tevens is de volgende wetgeving van toepassing:

- archiefwet;
 - algemene Wet Bestuursrecht;
 - kaderwet Zelfstandige Bestuursorganen;
 - uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
 - wet Open Overheid (Woo) (voorheen: Wet openbaarheid van bestuur (Wob)).
-

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 en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Verwerkingsdoeleinde	Categorie Persoonsgegevens	Bewaartermijn	Motivatie bewaartermijn
Logging	Controleren van medewerkers op hun activiteiten omtrent het inzien van de vragenlijsten.	Gewoon	Zie hieronder.	Zie hieronder.
Monitoring	Controleren van medewerkers op hun activiteiten omtrent het inzien van de vragenlijsten.	Gewoon	Zie hieronder.	Zie hieronder.

In de generieke Selectielijst van het ministerie van EZK uit 2012 wordt onder andere gesproken over de zogenaamde "Kritische Onderwerpen" of ook wel genoemd "Hotspots". Hotspots zijn gebeurtenissen of ontwikkelingen die een grote impact hebben op de relatie tussen de overheid en burgers of op burgers onderling. De archieven van het Instituut, inclusief rechtsvoorgangers en rechtsopvolgers zijn voorlopig aangewezen als "Hotspot". Dit houdt in dat alle archieven van het Instituut lange tijd bewaard moeten worden.

De gegevens die voortkomen uit de taak en bevoegdheden van het Instituut zijn, op advies van DIV-RVO van 26-04-2019, aangemerkt als 'Hotspot', waarbij de persoonsgegevens worden 'gearchiveerd in het algemeen belang'. Dit is een verdere verwerking ten opzichte van de initiële verwerkingsdoelen. Deze verdere verwerking wordt als verenigbaar beschouwd t.o.v. het initiële verwerkingsdoel ingevolge art. 5, eerste lid sub b, jo. art. 89, eerste lid AVG.

De loggingsbestanden in MIRA vallen hier ook onder. De loggingsbestanden in MIRA bevatten informatie over wie toegang heeft gehad tot het systeem, welke acties zijn uitgevoerd en wanneer dat is gebeurd. Ze spelen een belangrijke rol bij het toezicht op de verwerking van gegevens en kunnen worden gebruikt als bewijs in onderzoeken of geschillen. Omdat deze bestanden nauw verbonden zijn met de zaakdossiers over schadeclaims, geldt voor beide dezelfde bewaartermijn. Dit zorgt ervoor dat alle relevante gegevens beschikbaar blijven zolang de zaakdossiers als "Hotspot" worden aangemerkt.

De persoonsgegevens zijn te bewaren zolang ook de zaakdossiers waarin de schadeclaims worden behandeld tot de "Hotspot" worden gerekend. Indien in een later stadium anders wordt bepaald kunnen de persoonsgegevens in principe worden vernietigd als het pand waarop de schadeclaims rusten in andere handen over gaat. Voor dit moment is dat nog niet aan de orde.

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. Voeg aanvullende informatie toe in het tekstveld.

De rechtsgronden zijn:

- Toestemming
 - Voor toestemming is nodig dat deze op ondubbelzinnige wijze vrij wordt gegeven voor een specifieke verwerking.
Licht toe hoe hieraan wordt voldaan.
- Noodzakelijk voor de uitvoering van de overeenkomst
 - Hier moet sprake zijn van een overeenkomst met de betrokkene, geef aan van wat voor overeenkomst sprake is.

- Noodzakelijk om te voldoen aan een wettelijke verplichting
 - Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
- Noodzakelijk om de vitale belangen van de betrokkene of een ander te beschermen
 - Hiervan kan sprake zijn wanneer iemands leven of gezondheid in gevaar is en die persoon niet in staat is om toestemming te geven.
- Noodzakelijk voor de vervulling van een taak van algemeen belang
 - Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.
- Noodzakelijk voor de behartiging van een gerechtvaardigd belang
 - Deze grondslag is niet van toepassing op gegevensverwerkingen die worden uitgevoerd in het kader van de publieke taak van een overheidsorgaan.
 - Voor deze grondslag is een belangenafweging nodig, voeg deze toe aan de toelichting op de rechtsgrond.

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
Logging	Noodzakelijk voor de behartiging van een gerechtvaardigd belang.	Zie tekst hieronder.
Monitoring	Noodzakelijk voor de behartiging van een gerechtvaardigd belang.	Zie tekst hieronder.

Het Hof van Justitie van de Europese Unie heeft drie cumulatieve voorwaarden gesteld waaraan moet zijn voldaan opdat een verwerking van persoonsgegevens rechtmatig is op basis van een gerechtvaardigd belang. Deze voorwaarden zijn zorgvuldig geformuleerd om een balans te waarborgen tussen de rechten van betrokkenen en de belangen van de verwerkingsverantwoordelijke. Een gerechtvaardigd belang kan slechts worden aangenomen als aan alle drie de voorwaarden wordt voldaan. Dit betekent dat zowel het belang zelf, de noodzakelijkheid van de verwerking, als de afweging van belangen tegen elkaar moeten worden beoordeeld.⁵

Gerechtvaardigd belang

Het Instituut heeft een gerechtvaardigd belang bij de verwerking van persoonsgegevens van JZ-medewerkers, met name voor het raadplegen van dossiers van aanvragers. Dit belang bestaat uit het waarborgen van voldoende beveiliging van de bijzondere persoonsgegevens van aanvragers. Het betreft een belang dat niet alleen voor het Instituut zelf van belang is, maar ook in het voordeel is van de betrokken aanvragers. Dit belang is noodzakelijk om de vertrouwelijkheid en integriteit van gevoelige informatie te kunnen garanderen. Daarbij draagt het bij aan de naleving van wettelijke verplichtingen ten aanzien

⁵Autoriteit Persoonsgegevens, “Normuitleg grondslag ‘gerechtvaardigd belang’”, www.autoriteitspersoonsgegevens.nl, 1 november 2019.

van gegevensbescherming. Het gerechtvaardigd belang van het Instituut is daarom inherent aan het waarborgen van het vertrouwen van betrokkenen.

Noodzakelijkheid

De verwerking van persoonsgegevens moet noodzakelijk zijn voor de behartiging van dit gerechtvaardigde belang. Loggen is daarbij een essentiële beveiligingsmaatregel. Het Instituut is verplicht om de persoonsgegevens die worden verwerkt adequaat te beveiligen en de autorisaties zorgvuldig te beheren. Dit omvat het bepalen en vastleggen van toegangsrechten van medewerkers. Logging registreert gebeurtenissen in de systemen, zoals wie welke gegevens heeft verwerkt (bekeken of aangepast). Zonder deze maatregelen zou het risico op datalekken of misbruik van gegevens aanzienlijk groter zijn. Logging draagt daarmee direct bij aan het voorkomen van onrechtmatige toegang binnen de systemen van het Instituut. Het waarborgen van de veiligheid en integriteit van gegevens is daarom zonder logging niet haalbaar.

Door logbestanden bij te houden en regelmatig te controleren, kan het Instituut beveiligingsinbreuken sneller ontdekken. Bovendien stelt dit het Instituut in staat om na een beveiligingsincident gerichte maatregelen te nemen om de schade te beperken en toekomstige incidenten te voorkomen. Het monitoren van logs helpt ook bij het identificeren van trends die wijzen op structurele beveiligingsproblemen. Dit geeft het Instituut de mogelijkheid om proactieve maatregelen te nemen om kwetsbaarheden te mitigeren. Zo wordt niet alleen de veiligheid van gegevens gewaarborgd, maar wordt ook de algehele IT-infrastructuur versterkt.

Afweging belangen

De belangen, grondrechten en fundamentele vrijheden van betrokkenen mogen niet zwaarder wegen dan het gerechtvaardigde belang. Het belang van het Instituut en de aanvragers van het IMS om persoonsgegevens veilig te verwerken weegt zwaarder dan het belang van medewerkers bij het beperken van hun privacy door logging en monitoring. Belangrijk hierbij is dat het Instituut ervoor zorgt dat de inbreuk op de privacy van medewerkers tot een minimum wordt beperkt. Er worden daarom strikte protocollen gevolgd om te waarborgen dat alleen relevante gegevens worden verzameld en gebruikt. De verwerking van persoonsgegevens wordt daarnaast regelmatig geëvalueerd om te toetsen of deze nog steeds noodzakelijk is. Het Instituut hanteert transparantie als kernwaarde, zodat medewerkers inzicht hebben in hoe en waarom hun gegevens worden verwerkt. Dit draagt bij aan een gevoel van vertrouwen en begrip onder de medewerkers.

De ingevulde Persoonlijke Impact Analyse (PIA) kan uitsluitend worden ingezien door JZ-medewerkers. Om toegang te krijgen, moet de medewerker van JZ motiveren waarom inzage in de PIA noodzakelijk is. De gegevens over deze inzage worden opgeslagen, waaronder de naam van de medewerker, de opgegeven reden voor inzage, en de datum en het tijdstip van het verzoek. Deze redenen voor inzageverzoeken worden intern gemonitord. Dit biedt niet alleen een extra laag beveiliging, maar ook een duidelijke audit trail voor het geval er vragen ontstaan over specifieke inzageverzoeken. De registratie en monitoring van toegangsverzoeken zorgen ervoor dat het risico op misbruik tot een minimum wordt beperkt.

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 nationaal identificatienummer, beoordeel of dit is toegestaan.

Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Type bijzonder persoonsgegevens	Uitzonderingsgrond
Logging	n.v.t.	n.v.t.
Monitoring	n.v.t.	n.v.t.

Binnen het proces van logging en monitoring worden geen bijzondere persoonsgegevens van medewerkers verwerkt.

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. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
Logging	gewoon	Zie paragraaf 6.	Zie paragraaf 6.
Monitoring	gewoon	Zie paragraaf 6.	Zie paragraaf 6.

Deze verenigbaarheidstoets beoordeelt of de verdere verwerking van persoonsgegevens in het kader van logging en monitoring van medewerkers verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Deze toets wordt uitgevoerd op basis van artikel 6, lid 4 van de AVG. Dit artikel stelt dat verdere verwerking van persoonsgegevens alleen is toegestaan als het nieuwe verwerkingsdoel verenigbaar is met het oorspronkelijke doel. In dit geval wordt beoordeeld of het loggen en monitoren van medewerkers aansluit bij de verplichtingen uit de arbeidsovereenkomst.

Het verband tussen het oorspronkelijke doel en het nieuwe/toekomstige doel

Er is een direct verband tussen het oorspronkelijke doel, namelijk het naleven en uitvoeren van de arbeidsovereenkomst, en het nieuwe doel, namelijk het controleren van activiteiten. Beide doelen zijn gericht op het uitvoeren van de arbeidsovereenkomst en de hieruit voortkomende werkzaamheden. De

verwerking sluit daarom aan bij de oorspronkelijke bedoeling en kan als verenigbaar worden beschouwd.

De context waarin de gegevens zijn verzameld

De gegevens zijn verzameld in het kader van de arbeidsovereenkomst tussen werkgever en medewerker, waarbij de werkgever een gerechtvaardigd belang heeft bij naleving van afspraken en bedrijfsprocedures. Er bestaat een hiërarchische arbeidsrelatie tussen beide partijen, wat inhoudt dat controle mogelijk en soms noodzakelijk is om schending van interne regels te voorkomen. Medewerkers kunnen redelijkerwijs verwachten dat bepaalde activiteiten binnen hun werkcontext worden gemonitord, zolang dit transparant en proportioneel gebeurt.

De soort en aard van de gegevens

De gegevens betreffen persoonsgebonden loggegevens, zoals toegangstijden, gebruikersacties en het bekijken van specifieke vragenlijsten. Dit zijn alleen gewone persoonsgegevens en geen bijzondere of strafrechtelijk persoonsgegevens van de medewerkers.

De mogelijke gevolgen van de voorgenomen verdere verwerking

De verwerking beoogt het voorkomen en opsporen van ongeoorloofd gedrag. De verwerking kan invloed hebben op disciplinaire beslissingen. Dit betekent dat waarborgen noodzakelijk zijn om medewerkers te beschermen. Tegelijkertijd kunnen er negatieve gevolgen optreden, waaronder een mogelijke inbreuk op de privacy, een gevoel van wantrouwen bij medewerkers en een verminderde werktevredenheid. Om deze risico's te beperken, moet de verwerking transparant zijn, proportioneel plaatsvinden en uitsluitend worden gebruikt voor het beoogde doel.

Het bestaan van passende waarborgen

Logging en monitoring van medewerkers vindt uitsluitend plaats op basis van het Loggings- en Monitoringsbeleid. Alleen noodzakelijke gegevens worden verwerkt. Medewerkers zijn geïnformeerd over de verwerking via de interne privacyverklaring en kunnen gebruikmaken van hun AVG-rechten.

Conclusie

Na toetsing van de vijf criteria kan worden geconcludeerd dat de verdere verwerking van loggegevens en monitoring in lijn is met de oorspronkelijke doeleinden en verenigbaar is.

14. Noodzaak en evenredigheid

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

Zie onderdeel 11 voor de uiteenzetting van de noodzakelijkheidstoets.

Rechten van 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.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Privacyverklaring IMG medewerkers	
Recht op rectificatie en aanvulling	Privacyverklaring IMG medewerkers	
Recht op vergetelheid	Privacyverklaring IMG medewerkers	Niet van toepassing zolang er een wettelijke verplichting is om de persoonsgegevens te bewaren.
Recht op beperking van de verwerking	Privacyverklaring IMG medewerkers	
Recht op dataportabiliteit	Privacyverklaring IMG medewerkers	Niet van toepassing. Dit recht is gebaseerd op de wettelijke grondslag toestemming of uitvoeren van een overeenkomst (artikel 20 AVG).
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	Privacyverklaring IMG medewerkers	
Recht om bezwaar te maken	Privacyverklaring IMG medewerkers	
Recht op duidelijke informatie	Privacyverklaring IMG medewerkers	

De privacyverklaring voor medewerkers is beschikbaar op de intranetwebsite van het Instituut. In deze verklaring worden de rechten van betrokkenen uitgebreid toegelicht, waaronder het recht om hun privacyrechten uit te oefenen. Medewerkers kunnen hier terecht om informatie te vinden over hoe hun persoonsgegevens worden verwerkt, voor welke doeleinden, en hoe zij gebruik kunnen maken van hun rechten, zoals inzage, rectificatie, of verwijdering van hun gegevens.

Op dit moment is de vindbaarheid van deze privacyverklaring echter een aandachtspunt. In tegenstelling tot de algemene privacyverklaring, die prominent via een duidelijke knop op de publieke website van het Instituut beschikbaar is, ontbreekt een vergelijkbare, gemakkelijk toegankelijke link voor de privacyverklaring specifiek gericht op medewerkers. Dit kan leiden tot onduidelijkheid bij medewerkers die op zoek zijn naar deze belangrijke informatie.

Om de gebruiksvriendelijkheid te verbeteren en de naleving van privacywetgeving te waarborgen, is het van belang om de toegankelijkheid van de privacyverklaring voor medewerkers op de intranetwebsite te verhogen. Dit kan bijvoorbeeld door een opvallende knop of een aparte sectie te creëren die direct vanaf de startpagina van het intranet bereikbaar is.

Beschrijving en beoordeling risico's voor de betrokkenen

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

15. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij 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;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus **laag**, **'gemiddeld'** en **'hoog'**. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.

		Kans		
		laag	midden	hoog
Impact	hoog	laag	hoog	hoog
	midden	laag	midden	hoog
	laag	laag	laag	laag

*De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.

Voeg aanvullende informatie in het tekstveld toe.

Beschrijving risico	Kans	Impact	Risico-inschatting
Geen sanctiebeleid vastgelegd voor medewerkers die mogelijk misbruik maken van hun technische inzagerechten in MIRA.	Midden	Midden	Midden
De privacyverklaring voor medewerkers is niet makkelijk vindbaar, waardoor medewerkers	Midden	Midden	Midden

Beschrijving risico	Kans	Impact	Risico-inschatting
niet op de hoogte zijn van hun rechten			

Sanctiebeleid

Het ontbreken van een sanctiebeleid voor medewerkers die hun inzagerechten oneigenlijk gebruiken vormt een risico. Zonder een dergelijk beleid zijn er geen duidelijke consequenties, wat medewerkers minder ontmoedigt om hun toegang voor ongeoorloofde doeleinden te gebruiken.

Vindbaarheid van de privacyverklaring voor medewerkers

Het huidige beleid maakt de privacyverklaring voor medewerkers niet makkelijk toegankelijk. Dit kan leiden tot onduidelijkheid over welke persoonsgegevens worden verwerkt en voor welke doeleinden. Het verbeteren van de vindbaarheid en toegankelijkheid van deze verklaring draagt bij aan meer transparantie en vertrouwen onder medewerkers.

Maatregelen en restrisico's

In onderdeel 16 wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel 15 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.

16. 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.

Geef tot slot een conclusie over de restrisico's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Gebruik voor de inschattingen van de risico's de niveaus laag, 'gemiddeld' en hoog. Gebruikmaken van de bijbehorende kleuren is aan te raden.

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Medewerkers die mogelijk misbruik maken van hun technische inzagerechten in MIRA.	Het opstellen van een sanctiebeleid voor medewerkers die misbruik maken van hun inzagerechten.	laag	IMG Waardedaling en Immaterieel
Medewerkers weten niet wat hun privacyrechten zijn.	De privacyverklaring voor medewerkers duidelijker vindbaar maken met een knop op het intranet.	laag	Privacy

Ondertekening

Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	
Directie/afdeling verantwoordelijke(n)	
Functie verantwoordelijke(n)	
Datum ondertekening	
Handtekening	

5.1.2e

5.1.2e

23-1-2025

DPIA oplegger

Aanleiding

Het Instituut Mijnbouwschade Groningen (hierna: het Instituut) wil in 2025 de RijksRoosterApplicatie (hierna RRA) in gebruik nemen. Op de applicatie is al een rijksbrede DPIA uitgevoerd. Voor de ingebruikname van de applicatie bij het Instituut worden in deze DPIA oplegger de specifieke verwerkingen die het Instituut in de applicatie wil uitvoeren getoetst aan de beginselen uit de AVG.

Hierna worden eerst de onderdelen waarvoor aanvulling op de algemene DPIA nodig is besproken. De risico's en maatregelen uit de DPIA, en de eventuele aanvullingen op de Rijksbrede DPIA RRA worden daarna besproken.

Persoonsgegevens en betrokkenen

De RRA wordt binnen het Instituut niet voor alle medewerkers gebruikt. Enkel de medewerkers die structureel (meer dan 12 keer per jaar) buiten de standaard kantooruren (maandag t/m vrijdag tussen 8.00 – 18.00 uur) werken krijgen een medewerkers account in de RRA.

Binnen het IMG gaat het om de volgende medewerkers die hun rooster in de RRA kunnen vinden:

- Zaakbegeleiders
- Facilitair medewerker (steunpunten/inhuur via UZB)

Om dit mogelijk te maken krijgen een aantal groepen binnen het Instituut toegang tot de RRA. Het gaat om de volgende mensen:

- Functioneel beheerders: Beheer applicatie (zoals stamgegevens en functionele inrichting). Externe medewerker vanuit het Rijk, niet vanuit het Instituut.
- Planners: Maken/bijhouden van roosters
- Managers: Accorderen van verzoeken (mutaties, verlof, roosters)
- Medewerkers: Inzien rooster, aanvragen doen (mutaties, verlof)

Elke groep heeft vervolgens autorisaties die passen bij de werkzaamheden die zij in hun functie uit moeten kunnen voeren.

- DFB: Volledige autorisatie op organisatieniveau.
- Planner: Recht om roosters te maken/wijzigen voor geselecteerde plangroep(en) (afdeling/team) (NB. dit is niet onze medewerker Planning zoals wie die kennen binnen het team Planning van KCDV)
- Manager: Recht om roosters te bekijken en mutaties te beoordelen voor geselecteerde plangroep(en). Managers kunnen aanvragen accepteren en afwijzen en roosters bekijken en controleren en gerealiseerde roosters goedkeuren
- Medewerkers: Recht om eigen rooster te bekijken en mutaties aan te vragen

Binnen de applicatie worden de volgende persoonsgegevens verwerkt wanneer je een account hebt:

Naam, (zakelijk)e-mailadres, functie en wachtwoord(Net als P-direkt met SingleSign On)

Van de mensen die een account hebben voor de applicatie omdat zij vallen binnen de rooster doelgroep worden in de applicatie aanvullend de volgende persoonsgegevens verwerkt:

Werktijden, (on)beschikbaarheid, afwezig, alle vormen van afwezigheid(bv, ziekte, verlof etc.) worden afgeschermd in de RRA.

Uit de Rijksbrede DPIA Rijks Rooster Applicatie volgen een aantal risico's, waar ook maatregelen voor geformuleerd zijn. Specifiek zijn voor het Instituut de volgende risico's met bijbehorende maatregelen in het bijzonder relevant:

- Fouten in autorisaties kunnen leiden tot uitgebreide toegankelijkheid. Als maatregel moet het Instituut hierom periodiek de autorisatiematrix herzien.
- Er kan een voorkeursbehandeling ontstaan bij het inwilligen van roosterwensen. Planners dienen hiervan bewust te worden gemaakt en er dient een controle plaats te vinden door de managers.
- Op dit moment worden medewerkers nog niet geïnformeerd over deze verwerking in de interne privacyverklaring van RVO. Deze privacyverklaring dient dan ook te worden aangevuld.
- Het Instituut verwerkt minder persoonsgegevens dan dat de RRA volgens de rijksbrede DPIA kan verwerken. Hierdoor bestaat het risico dat het Instituut op termijn meer persoonsgegevens gaat opnemen in de RRA dan origineel beoordeeld is in deze oplegger. Het privacyteam dient dan ook te worden ingeschakeld, zodra de wens bestaat om meer persoonsgegevens te verwerken dan in deze oplegger is beoordeeld.

Betreft: FG advies DPIA RRA

Auteur: 5.12e Functionaris Gegevensbescherming

Datum: 26-03-2025

Aanleiding

In 2025 wil het Instituut Mijnbouwschade Groningen (hierna: "het Instituut") gebruik maken van de Rijks Rooster Applicatie (hierna: "RRA"). Via deze applicatie kan het Instituut voor een aantal groepen medewerkers een rooster opstellen. Het gaat hierbij om de zaakbegeleiders en facilitair medewerkers die 12 keer per jaar of meer buiten de kantooruren werkzaam zijn.

De RRA komt voort uit het programma "Het Nieuwe Roosteren" waar in het verleden een DPIA op uitgevoerd is. Op de RRA is door Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: "het Ministerie") nu ook een DPIA uitgevoerd en het Instituut heeft een "oplegger" opgesteld om de DPIA te concretiseren naar de gegevensverwerkingen die door het Instituut in de RRA worden uitgevoerd. De rijks DPIA met de oplegger van het Instituut worden in dit advies als geheel beschouwd en aangehaald als de DPIA.

In de DPIA wordt niet beschreven waarom een DPIA noodzakelijk is. De RRA verwerkt voor de rijks organisaties structureel en op grootschalige wijze persoonsgegevens. Daarnaast wordt in het proces verschillende datasets met elkaar samengevoegd. Tot slot bestaat er de mogelijkheid om gebruik te maken van automatische besluitvorming. Hierdoor wordt aan drie van de negen voorwaarden van de Autoriteit Persoonsgegevens (hierna: "AP") over het moeten uitvoeren van een DPIA voldaan. Voor het Instituut wordt niet op grote schaal persoonsgegevens verwerkt door het beperkte aantal betrokkenen. Daarnaast wordt ook geen gebruik gemaakt van de optie om automatische besluitvorming te realiseren. Hierdoor wordt aan maar één van de voorwaarden van de AP voldaan, waardoor het uitvoeren van een DPIA door het Instituut op de RRA niet noodzakelijk. Het is daarentegen wel verstandig om een DPIA hierop uit te voeren zodat hier de risico's geanalyseerd worden en de juiste maatregelen genomen worden om de risico's te mitigeren.

Doel van het gewenste proces

Het Instituut wenst gebruik te maken van de RRA om zo niet alleen een rooster voor de zaakbegeleiders en facilitair medewerkers die buiten kantooruren werken op te stellen, maar ook verzuim en verlof te registreren. Het Instituut kan hierdoor een sluitend operationele planning opstellen waardoor de juist gekwalificeerde betrokkenen de functies buiten de kantooruren kunnen vervullen.

Aandachtspunten/risico's