Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Bescherming persoonsgegevens IMG

Definitief

Colofon

Titel	Bescherming persoonsgegevens IMG
Uitgebracht aan	Dhr. mr. H.C.D. Korvinus
Datum	9 juli 2024
Kenmerk	2024-0000378005

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

IMG zet stappen om de bescherming van persoonsgegevens naar een hoger niveau te brengen, lange termijn operationele borging vraagt aandacht

Het Instituut Mijnbouwschade Groningen (IMG) heeft naar aanleiding van een volwassenheidsscan in 2021 en het datalek in het najaar van 2022 op korte termijn een aantal stappen gezet om de bescherming van persoonsgegevens beter te borgen binnen de organisatie. Wij hebben vastgesteld dat deze stappen hoofdzakelijk hebben plaatsgevonden in opzet; het beschrijven van beleidsstukken hoe het IMG omgaat met de bescherming van persoonsgegevens. Gezien het recente karakter van menig beleidsstuk (gemaakt of gewijzigd in 2023), hebben wij de operationele uitvoering als zodanig nog niet altijd aangetroffen.

Op het gebied van controle- en monitoringsactiviteiten is aandacht noodzakelijk. Wij hebben bij meerdere onderwerpen vastgesteld dat het in de praktijk ontbreekt aan structurele controle- en monitoringactiviteiten waardoor het IMG geen actueel en volledig inzicht heeft in de verschillende privacyrisico's die het IMG loopt en mogelijk te laat detecteert. De activiteiten die plaatsvinden zijn ad hoc. Dit geldt onder andere voor onderwerpen als het register van verwerkingsactiviteiten en het uitvoeren en hoofdzakelijk opvolgen van de noodzakelijke maatregelen voorkomend uit de Data Protection Impact Assessments (DPIA's).

Op het gebied van beveiliging hebben wij ook de beschreven processen en procedures nog niet altijd als zodanig aangetroffen in de praktijk. Met name de expliciete koppeling met privacy komt niet altijd duidelijk naar voren. Dit geldt onder andere voor onderwerpen als identiteit en toegangsbeheer, veilige gegevensoverdracht en encryptie. Concrete passende technische en organisatorische maatregelen gekoppeld aan privacy die genomen dienen te worden om de beveiliging van persoonsgegevens te waarborgen zijn niet altijd even duidelijk beschreven en/of aangetroffen in de praktijk. Dit neemt echter niet weg dat het IMG wel algemene beveiligingsmaatregelen treft alsmede DigiD-assessments en pentesten op de belangrijkste systemen uitvoert.

Lange termijn borging van de bescherming van persoonsgegevens binnen het IMG vraagt om aandacht. Niet alleen vanwege het recente karakter van menig beleidsstukken, vastgestelde verschillen tussen deze beleidsstukken en operationele werkelijkheid (met name op het gebied van controle en monitoring) maar ook vanwege de personele bezetting aangaande privacy-gerelateerde taken. Gezien de aard van de organisatie is veel sprake van (tijdelijke) inhuurkrachten. Dit heeft ervoor gezorgd dat het IMG weliswaar op korte termijn stappen heeft kunnen zetten naar een hoger volwassenheidsniveau maar daarin verschuilt ook het risico dat wanneer de inhuurperiode eindigt, kennis en expertise het IMG verlaat. Dit zet de lange termijn operationele borging van de bescherming van persoonsgegevens onder druk. Juist op dit gebied zijn verbeteringen binnen het IMG noodzakelijk.

1 Inleiding opdracht

1.1 Aanleiding opdracht

Het Instituut Mijnbouwschade Groningen (IMG) heeft in het najaar van 2022 twee datalekken geconstateerd in de webapplicatie MijnDossier, het aanvraagsysteem voor burgers. Door misbruik te maken van een kwetsbaarheid in de applicatie heeft in een geval een commerciële partij via de website (na het inloggen met DigiD/e-Herkenning en zich voor te doen als eigenaar, erfgenaam, of gemachtigde) adressen verzameld van gedupeerden om potentiële cliënten te werven.

Na dit geconstateerd te hebben, heeft het IMG extern onderzoek door het Nederlands Forensisch Incident Response (NFIR) laten uitvoeren naar de betreffende kwetsbaarheid. Hierbij is vastgesteld dat in de 23 testscenario's geen datalekken geconstateerd zijn, maar kon niet worden uitgesloten dat er geen andere datalekken bestaan in Mijn Dossier. Het NFIR heeft daarom aanbevolen een uitgebreide penetratie test uit te laten voeren om de beveiligingsaspecten en de privacyaspecten te testen.

Naar aanleiding van het datalek en een publicatie hierover in de media zijn er schriftelijke Kamervragen gesteld en is de motie 33529-1093 ingediend en aangenomen. De motie verzoekt om de databescherming bij het IMG te laten doorlichten en de Kamer hierover te informeren. De ADR is verzocht het onderzoek uit te voeren naar de bescherming van de (bijzondere) persoonsgegevens door IMG.

1.2 Hoofdvraag en deelvragen

Dit onderzoek geeft antwoord op de hoofdvraag: welke kwetsbaarheden worden onderkend die de bescherming van (bijzondere) persoonsgegevens, zoals omschreven in de motie 33529-1093 rondom de selectie verwerkingen kunnen belemmeren? De hoofdboodschap op pagina 4 geeft hier antwoord op.

Het antwoord op de hoofdvraag komt voort uit hoofdstuk 2 waarin aan de hand van de onderwerpen uit het Privacy Controle Framework (PCF) de deelvragen zijn behandeld:

1. Welke organisatorische beheersmaatregelen heeft IMG getroffen teneinde de bescherming van (bijzondere) persoonsgegevens omtrent de geselecteerde privacymanagement aspecten te borgen?
2. Welke activiteiten heeft IMG geïnitieerd om het interne bewustzijn omtrent informatiebeveiliging en privacyvraagstukken te vergroten?
3. Welke technische beheersmaatregelen heeft IMG getroffen teneinde de bescherming van (bijzondere) persoonsgegevens omtrent de geselecteerde privacymanagement aspecten borgen?
4. Welke restrisico's worden onderkend bij de huidige inrichting van het stelsel van beheersmaatregelen omtrent de geselecteerde privacymanagement aspecten?

De specifieke verwijzing van deelvragen, PCF-onderwerpen gekoppeld aan de paragrafen is te vinden in bijlage 1.

1.3 Context

Het IMG is een zelfstandig bestuursorgaan (ZBO) ressorterend onder het ministerie van EZK. Zij heeft een bestuur en een ondersteunende organisatie. Het bestuur stelt de werkwijze vast en neemt besluiten over de individuele aanvragen. IMG onderkent de volgende ondersteunende afdelingen:

- Zaakbegeleiders

- Serviceloket
- Schade-afhandeling
- Staf en ondersteunende diensten

Vanuit de maatschappij, politiek en media is er veel aandacht voor de opdracht en uitvoering van de taak van het IMG. Een van de doelstellingen van het IMG is zorg te dragen voor de correctheid en bescherming van (bijzondere) persoonsgegevens zoals zij die binnen de gestelde kaders verwerkt. De bescherming van deze (bijzondere) persoonsgegevens dient in overeenstemming te zijn met de eisen die door de Algemene Verordening Gegevensbescherming (AVG) worden gesteld.

Voor haar bedrijfsvoering en informatievoorziening maakt het IMG voor een groot deel gebruik van de diensten van de Rijksdienst voor Ondernemend Nederland (RVO) en DICTU. RVO heeft het IMG ook lange tijd ondersteund op het gebied van informatiebeveiliging. Vanwege de groei van de taak van de organisatie en de bijbehorende grotere behoefte aan informatievoorziening heeft het IMG in 2021 Informatievoorziening (IV) formeel vormgegeven. In het verlengde van de vormgegeven IV-organisatie is er gedurende 2021 een professionaliseringsslag geweest op het gebied van Informatiebeveiliging en Privacy (IB&P) en zijn een CISO en Privacy Officer aangesteld. In 2022 is het vastgestelde IB&P beleid uitgewerkt en ten uitvoer gebracht in de verschillende jaarplannen.

2 Bevindingen opdracht

2.1 Privacybeleid aanwezig, aandacht voor privacy by design/default en controle hierop bij actualisatie privacybeleid benodigd

Wij hebben vastgesteld dat het IMG beschikt over een beschreven privacybeleid, vastgesteld begin 2022. Het privacybeleid is intern via het intranet beschikbaar gesteld. De privacyverklaring is extern via de website van het IMG gepubliceerd. In het privacybeleid staat beschreven op welke manier het IMG omgaat met de bescherming van persoonsgegevens, dan wel de beheersing van privacyrisico's. Jaarlijks legt het IMG met een self-assessment verantwoording af aan de Chief Information Officer (CIO) van EZK over de navolging van de maatregelen uit de privacy baseline EZK. Aangegeven is dat het IMG inzichtelijk heeft waar verbetering noodzakelijk is als het gaat om de implementatie van de normen uit het NOREA PCF. Qua privacy-volwassenheidsniveau zit het IMG volgens het self-assessment over het jaar 2022 op niveau 2 (herhaalbaar)/niveau 3 (gedocumenteerd) op een schaal van nul tot en met vijf.

Beschreven is dat het privacybeleid eens per jaar of bij wijzigingen in wet- en regelgeving, de missie, visie of strategie van IMG wordt geëvalueerd en waar nodig bijgesteld of herzien. Naar aanleiding van het datalek in de zomer van 2022 (en andere constateringen uit het self-assessment over het jaar 2022) is het privacybeleid niet geëvalueerd of herzien. Dit geldt tevens voor het jaar 2023. In het jaarplan voor 2024 staat wel als actiepunt opgenomen om het privacybeleid aan te vullen. Aangegeven is dat het IMG wel regelmatiger de publieke privacyverklaring updatet. Wij hebben vastgesteld dat de privacyverklaring meerdere keren in 2023 is geactualiseerd.

In de zomer van 2021 is door het MT besloten dat nieuwe projecten en programma's niet starten voordat helder is wat de impact is op de informatievoorziening en het IT-landschap. Aangegeven is dat wanneer binnen het IMG een nieuw proces wordt gestart waarbij persoonsgegevens worden verwerkt, het team IB&P benaderd dient te worden voor advies en een toets op de rechtmatige grondslag. Deze verwevenheid van IB&P binnen de project startarchitectuur (PSA) is echter niet als zodanig beschreven evenals de manier waarop aspecten rondom privacy by design en default tot uiting komen. Dit geldt ook voor de manier waarop controle wordt gehouden tijdens en na de uitvoering.

2.2 Rollen en verantwoordelijkheden privacyactoren beschreven, in praktijk echter niet altijd operationeel op het gebied van controle en monitoring

Het IMG heeft de taken, bevoegdheden en verantwoordelijkheden rondom de beheersing van privacyrisico's beschreven. Rollen en verantwoordelijkheden zijn per functionaris beschreven, ondersteunt door een organogram van het IMG. Hierbij is tevens op papier een onderscheid beschreven tussen eerste lijn (bestuur en management), tweede lijn (Privacy Officers) en derde lijn (interne controle). Aangegeven is dat Privacy Officers uit de tweede lijn ook adviseurs zijn van de eerste lijn. Het IMG heeft als doel om in 2024 ook in de eerste lijn eigen IB&P contacten te hebben. Rollen en verantwoordelijkheden rondom het afsluiten van verwerkersovereenkomsten zijn in opzet beschreven. Het IMG beschikt ook in bestaan over een overzicht met daarin de afgesloten verwerkersovereenkomsten.

Bezetting en capaciteit is een uitdaging binnen het IMG. Wij hebben vastgesteld dat veel privacy-gerelateerde rollen en verantwoordelijkheden worden bekleed door (tijdelijke) inhuurkrachten. Dit is mede in gang gezet naar aanleiding van het

datalek in het najaar 2022 en de publieke aandacht die daarmee gepaard ging. Ten tijde van het onderzoek hebben wij vastgesteld dat het aantal privacy-gerelateerde collega's in vast dienstverband (met uitgebreidere kennis over het instituut) in de minderheid is en afneemt. Alhoewel inhuurkrachten op korte termijn bijdragen aan een ontwikkeling naar een hoger volwassenheidsniveau en passen bij de aard van de organisatie, kan op lange termijn de borging van kennis en expertise binnen het IMG in de knel komen. In opzet (beschreven procedures) hebben wij verbeteringen vastgesteld. Bestaan (uitvoering van die beschreven procedures) loopt echter op bepaalde onderwerpen nog achter. Zolang nog niet alle privacy-gerelateerde processen én controles daarop structureel zijn ingericht (zie jaarlijkse self-assessment i.v.m. volwassenheidsniveau), loopt het IMG een risico betreft lange termijn borging van privacykennis en privacybeheersing.

Structurele controle en monitoring vanuit de derde lijn is een aandachtspunt voor het IMG en past bij een hoger volwassenheidsniveau waar het IMG naar streeft. Weliswaar is beschreven dat het kwaliteitsteam en de adviseurs interne controle of auditors toezicht dienen te houden op de processen binnen het IMG waarmee privacy verbonden is. Dit hebben wij echter als zodanig niet vastgesteld. Dit geldt tevens voor de uitvoering van toezichtwerkzaamheden van de Functionaris Gegevensbescherming (FG). Mede door functiewisselingen en tijdelijke inhuur is het intern toezicht vanuit de FG nog niet volledig ingericht. De FG heeft ook geen jaarverslag uitgebracht over het jaar 2022.

2.3 Register van verwerkingsactiviteiten biedt nog geen actueel en volledig beeld, controle en monitoring op basis hiervan nog niet mogelijk

Het IMG identificeert en documenteert verwerkingen van persoonsgegevens aan de hand van een AVG-register (breed bekend als de EZK-tool) ondersteunt door een in opzet beschreven functioneel handboek. Het handboek beschrijft hoe de applicatie werkt bij het invoeren en muteren van een verwerking evenals de taken en verantwoordelijkheden rondom het AVG-register. Om het register actueel, inhoudelijk juist, volledig en samenhangend te houden beschikt IMG over een in opzet beschreven PDCA-procedure. Aangegeven is dat het register van verwerkingsactiviteiten echter niet actueel is omdat er onvoldoende capaciteit beschikbaar is om de beschreven PDCA-procedure als zodanig uit te voeren. Met de (tijdelijke) inhuur in 2023 zijn door het IMG stappen ondernomen om het register verder te vullen als onderdeel van het jaarplan 2023. Actieve controle van het register zelf en op basis van het register staat gepland in een later stadium en wordt momenteel nog niet uitgevoerd.

Door een steekproef van vijf verwerkingen hebben wij vastgesteld dat één van de vijf verwerking definitief is vastgesteld. De andere zijn nog in bewerking omdat de DPIA's nog niet zijn afgerond of door wijzigingen in wet- en regelgeving. Bij iedere verwerking staat welke gegevens worden verwerkt en indien noodzakelijk of het bijzondere categorieën van persoonsgegevens betreft wat volgens de entries bij drie verwerkingen het geval is. In het privacybeleid staan echter geen uitgangspunten en uitzonderingsgronden beschreven rondom de verwerking van bijzondere categorieën van persoonsgegevens.

2.4 Bewustwordingsactiviteiten uitgevoerd maar vrijblijvend van aard

Privacy-gerelateerde activiteiten en werkzaamheden worden mede gezien de aard van de organisatie over het merendeel uitgevoerd door (tijdelijke) inhuurkrachten. Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier het IMG op lange termijn deze uitdaging aan gaat (beschreven wervingsplan en -behoefte) en maakt dan ook geen onderdeel van het privacyjaarplan voor 2023. Aangegeven is dat de Privacy Officers binnen het IMG een passende opleiding hebben afgerond en de meeste over adequate privacy-gerelateerde certificeringen beschikken.

Naast het uitbreiden van privacykennis door werving is het van belang dat medewerkers die vanuit hun functie normaliter over minder privacykennis beschikken, bewust worden van privacyrisico's in hun werk en daar ook training in volgen. In het privacybeleid staat beschreven dat in samenwerking met de CISO en IMG Academie het bewustwordingsprogramma IB&P wordt opgesteld en uitgevoerd. Hierbij wordt zoveel mogelijk aangesloten op de rijksbrede initiatieven. Wij hebben vastgesteld dat het IMG in de jaren 2022 en 2023 bewustwordingsactiviteiten heeft uitgevoerd waaronder e-learning, berichten op intranet en e-mails.

Privacybewustwording binnen het IMG is wel nog groeiende en vrijblijvend van aard. Er is bijvoorbeeld geen verplichte (jaarlijkse) training en het toezien op de naleving van het bewustwordingsprogramma door de FG zoals is beschreven in het privacybeleid, hebben wij niet vastgesteld. Het IMG hoopt door nadrukkelijkere aandacht voor privacy het vertrouwen en aanzien van de burger in het instituut te herstellen en te waarborgen.

2.5 Privacyrisicomanagement vraag extra aandacht, in het bijzonder uitvoering en opvolging noodzakelijke maatregelen DPIA's alsmede controle daarop

Het IMG heeft in het privacybeleid beschreven dat (risicovolle) verwerkingen van persoonsgegevens alleen mogen plaatsvinden als er een risicoanalyse is uitgevoerd. Het privacybeleid verwijst naar de PDCA-cyclus en andere activiteiten ten behoeve van de beheersing van privacyrisico's. Deze activiteiten hebben wij echter niet allemaal zoals beschreven is volledig aangetroffen in de praktijk. Dit geldt tevens voor een beschrijving van criteria waarop privacyrisco's worden vastgesteld, geaccepteerd en gedocumenteerd. Wij hebben ook geen beschrijving aangetroffen voor toezichts- en monitoringsactiviteiten om bij wijzigingen van risico's en risicobeheerstrategieën deze opnieuw te beoordelen. Wel hebben wij het bestaan van de uitvoering van de self-assessment als zodanig vastgesteld.

Het IMG beschikt over een beschreven DPIA-procedure. Beschreven is dat bij de start van een project een uitgewerkte Project Startarchitectuur is vereist waarin middels een pre-DPIA (QuickScan) security en privacyrisico's geïdentificeerd dienen te worden. Aangegeven is dat een pre-DPIA (QuickScan) niet wordt uitgevoerd indien het evident is dat een DPIA noodzakelijk is. Vastgesteld door middel van een steekproef en aangegeven tijdens interviews, is dat binnen het IMG nog niet alle DPIA's zijn afgerond. Van de DPIA's die zijn afgerond hebben wij vastgesteld dat het Rijksbrede format wordt gehanteerd en de vereiste informatie bevat.

Het monitoren en toezichthouden op de uitvoering van de DPIA zelf alsmede de uit de DPIA voortkomende benodigde technische en organisatorische maatregelen, is een blijvend aandachtspunt binnen het IMG. Het IMG heeft in de DPIA-procedure beschreven dat genomen maatregelen op gezette tijdstippen getest, beoordeeld en geëvalueerd dienen te worden op doeltreffendheid. Dit zorgt ervoor dat de maatregelen op alle momenten tijdens de verwerking passend blijven. Voor de verwerkingen die wij hebben geselecteerd hebben wij deze controle en monitoring niet als zodanig aangetroffen in de praktijk.

2.6 Datalekkenprocedure beschreven en adequaat opgepakt, repeterend karakter datalekken valt op

Het IMG beschikt over een beschreven werkinstructie en procedure (augustus 2023) gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. In de procedures staan taken en verantwoordelijkheden beschreven, de escalatieprocedure ondersteunt door een beslisboom en het melden indien noodzakelijk aan de toezichthoudende autoriteit en/of betrokkene(n). Daarnaast is beschreven dat ongeacht of een inbreuk aan de toezichthoudende autoriteit en/of de betrokkenen moet worden gemeld, deze altijd intern gedocumenteerd zal moeten worden. Wij hebben vastgesteld dat het IMG beschikt

over een register datalekken. In het register van datalekken worden in de basis de vereiste gegevens gedocumenteerd die de AVG stelt aan dit register. Informatie over de (tijdigheid van de) melding aan de Autoriteit Persoonsgegevens (AP) en de betrokkene is echter niet altijd volledig duidelijk in het register.

Op basis van het register hebben wij een steekproef uitgevoerd op datalekken die hebben plaatsgevonden in 2023. De geselecteerde datalekken zijn tijdig en adequaat opgepakt en tevens indien nodig gemeld aan de AP en middels een brief aan de betrokkenen. Hierbij dient wel een kanttekening te worden gemaakt dat bij enkele datalekken het datalek al een bepaalde periode plaatsvond voor constatering door het IMG. Maatregelen voorkomend uit het datalek om soortgelijke datalekken in de toekomst te voorkomen, zijn echter niet altijd beschreven. De aangeleverde correspondentie van de datalekken uit de steekproef in combinatie met het register stelt de AP wel in staat de naleving van artikel 33.5 te controleren.

Bij het inspecteren van het register van datalekken valt het op dat het merendeel van de datalekken eenzelfde soort datalek betreft; het versturen of afgegeven van persoonsgegevens aan verkeerde ontvanger of het koppelen van een document met persoonsgegevens aan een dossier van een andere burger die daar inzicht in heeft. Het betreft een handmatige handeling. Aangegeven is dat het een menselijke fout is en dat technische en organisatorische maatregelen dit niet kunnen oplossen. Het IMG heeft hier middels een bericht op intranet aandacht aan besteed maar heeft niet voorkomen dat soortgelijke datalekken niet meer plaatsvinden.

2.7 Uitwerking van concrete beveiligingsmaatregelen gekoppeld aan privacy niet altijd even duidelijk

2.7.1 Programma van Informatiebeveiliging

Het IMG heeft een informatiebeveiligingsbeleid op strategisch niveau vastgesteld waarin de ambities zijn beschreven op het gebied van informatiebeveiliging. In dit beleid is ook de relatie opgenomen met het privacybeleid. Indien één van deze beleidskaders wijzigt, wordt expliciet getoetst of dit in lijn is met de andere beleidskaders. In het strategisch informatiebeveiligingsbeleid worden geen concrete passende technische en organisatorische maatregelen benoemd die genomen dienen te worden om de beveiliging van persoonsgegevens te waarborgen. Het niet adequaat beschermen van persoonsgegevens kan leiden tot onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals een hack of andere poging tot het verkrijgen van ongeautoriseerde toegang.

In de periodieke risicobeoordelingen die het IMG uitvoert, komt privacy aan de orde. Deze worden middels een standaard format uitgevoerd. In opzet is in het strategisch beveiligingsbeleid vastgelegd dat de lijnmanager periodiek de betrouwbaarheidseisen en beveiligingsmaatregelen evalueert en bijstelt waar nodig. Daarnaast is vastgelegd dat er jaarlijks zowel interne- als externe beveiligings-onderzoeken dienen te worden uitgevoerd zoals DigiD-assessments en pentesten op de belangrijkste systemen. Uit aangeleverde overzichten blijkt ook dat er jaarlijks een pentest wordt gedaan op Mira en Atabix.

2.7.2 Identiteit en Toegangsbeheer

Voor het verlenen van toegang tot systemen zijn procesbeschrijvingen opgesteld waarin beschreven is op welke wijze gebruikers toegang krijgen tot gegevens. Uit deze procesbeschrijvingen blijkt niet dat deze zijn opgesteld vanuit een privacy oogpunt. Zo zijn deze bijvoorbeeld niet gebaseerd op de gevoeligheid van de gegevens. Periodiek wordt gecontroleerd of de personen die autorisaties hebben om gegevens te raadplegen deze ook behoren te hebben. Verantwoordelijk voor deze controle zijn de diverse teamleiders.

Voor toegangsdetectie en monitoringssystemen met betrekking tot toegangsbeheer is er in opzet wel een beleid aangetroffen, maar zijn er geen concrete procedures aangetroffen. Wat betreft de operationele keuzes met betrekking tot de inrichting van het identiteit- en toegangsbeheer (zoals wachtwoordbeleid) worden DICTU en de RVO gevolgd. Er blijkt echter niet dat formele procedures die het IMG zelf in plaats zou moeten hebben ook zijn ingericht. Het risico bestaat dat het IMG zelf geen duidelijk beeld heeft van welke zaken de verantwoordelijkheid zijn van DICTU, en voor welke onderdelen (en procedures) zij zelf verantwoordelijk zijn.

Aangegeven is dat het IMG bezig is met het opstellen van een tactisch informatiebeveiligingsbeleid waarin procedures omtrent toegangsbeheer worden omschreven.

2.7.3 Veilige gegevensoverdracht

Het IMG classificeert gegevens op basis van gevoeligheid en benodigde niveaus van (toegangs-)bewaking bij gegevensoverdracht. Zo wordt de classificatie van gegevens meegenomen in de QuickScan. Taken- en verantwoordelijkheden voor het IMG zijn op hoofdlijnen beschreven m.b.t. het gebruik van de Rijkszaak Applicatie van DICTU. Hierin zijn echter geen specifieke beveiligingsmaatregelen aangetroffen. Er zijn geen afspraken aangetroffen over welke beheeractiviteiten de IT-organisatie van het IMG moet uitvoeren en aan welke eisen zij moeten voldoen. Er zijn dan ook geen specifieke maatregelen voor het behandelen (waaronder versturen) van persoonsgegevens, gebruik van externe verbindingen en gebruik van draadloze netwerken aangetroffen.

2.7.4 Versleuteling en eindpuntbeveiliging

Wij hebben vastgesteld dat versleutelingstechnologieën (encryptie) niet op elke vorm van data op het hetzelfde niveau wordt toegepast, nu er afwijkingen bestaan op de opgeslagen data (data at rest). Nu versleutelingstechnologieën niet consequent worden toegepast bestaat het risico dat data, bijvoorbeeld die in verouderde systemen, ingezien of gewijzigd kan worden door onbevoegden.
Het uitgangspunt voor het toepassen van versleutelingstechnologieën is het beleid van EZK, aangevuld met handreikingen en adviezen door het NCSC. Specifieke beleidsregels en procedures voor het IMG in relatie tot opslag van (persoons)gegevens op draagbare media of specifieke categorieën van apparaten zijn niet aangetroffen. Het gebrek aan specifieke procedures met betrekking tot het toepassen van versleuteling bij de systemen binnen het IMG maakt het mogelijk dat afwijkingen ontstaan.

2.7.5 Registreren van toegang

Hoewel er wel een logging- en monitoringsbeleid is opgesteld in 2021, hebben we niet aangetroffen dat het IMG proactief logt en monitort. Logs worden wel gebruikt om incidenten op te kunnen lossen en achteraf vragen te kunnen onderzoeken, maar er is geen sprake van een proactief proces van monitoring om inbreuken met betrekking tot persoonsgegevens te kunnen detecteren en te kunnen voorkomen. Hierdoor loopt het IMG het risico dat inbreuken in verband met persoonsgegevens en pogingen om ongeautoriseerde toegang te verkrijgen niet tijdig worden gedetecteerd.

Ook voor het proces van logging en monitoring geldt dat, hoewel in het beleid wordt verwezen naar een procedurebeschrijving voor logging (en raadplegen van logs), er geen beschreven werkinstructie of procedure is aangetroffen. Ook het risicomanagementbeleid waarnaar wordt verwezen in het logging- en monitoringbeleid is ten tijde van het onderzoek niet aangetroffen.

2.8 Bewaarbeleid en -termijnen nog niet vastgesteld

Ten tijde van het onderzoek hebben wij geen selectielijst aangetroffen alsmede een bewaarbeleid. Dit betekent dat er geen persoonsgegevens zijn verwijderd of

vernietigd. Voor het ministerie van EZK geldt vanaf 1 januari 2024 een vernieuwde selectielijst. Het IMG is hierin met haar taakuitvoering opgenomen. Aangegeven is dat de selectielijst nog wel via de officiële procedures en kanalen moet worden vastgesteld. Het IMG geeft aan de selectielijst wel alvast in te kunnen zetten waardoor bewaartermijnen aan informatie en gegevens die worden verzameld binnen het IMG toegekend kunnen worden.

3 Aanbevelingen en/of vervolgstappen

Op basis van de bevindingen weergegeven in hoofdstuk 2, doen wij de volgende aanbevelingen:

- Herzie het privacybeleid en besteed hierbij expliciet aandacht aan uitgangspunten rondom privacy by design/default alsmede de controle hierop.
- Beschrijf in het privacybeleid aanvullende uitgangspunten en uitzonderingsgronden om bijzondere categorieën van persoonsgegevens te mogen verwerken. Besteed hierbij tevens aandacht aan noodzakelijke technische en organisatorische maatregelen die deze verwerking mogelijk kunnen maken.
- Draag zorg voor voldoende capaciteit en aandacht om controle en monitoringsactiviteiten uit de derde lijn te laten uitvoeren.
- Realiseer het voornemen om het register van verwerkingsactiviteiten voor de uitvoeringen van regelingen verder te vullen om uiteindelijk controle en monitoring op basis van het register te kunnen bewerkstelligen.
- Maak bewustwordingsactiviteiten verplicht zodat iedere medewerker aantoonbaar groeit op het gebied van privacy en gegevensbescherming.
- Maak privacy-gerelateerde wervingsplan en -behoefte onderdeel van het jaarplan om op lange termijn privacykennis en -expertise te borgen binnen het IMG.
- Beschrijf criteria op basis waarvan privacyrisico's worden vastgesteld, geaccepteerd en gedocumenteerd.
- Realiseer het voornemen om de resterende DPIA's op korte termijn af te ronden.
- Besteed extra aandacht aan het monitoren en toezichthouden op de uitvoering van de uit de DPIA voortgekomen noodzakelijk technische en organisatorische maatregelen.
- Breid het register van datalekken uit met datum en tijd melding AP en/of betrokkenen alsmede benodigde bijlages om controle op basis van het register mogelijk te maken.
- Beschrijf en koppel aan de diverse beleidstukken welke privacy-specifieke technische en organisatorische maatregelen genomen (dienen te) worden.
- Stel procedures op, op basis van vastgesteld beleid, voor het versleutelen van gegevens, logging en voor toegangsdetectie en monitoringssystemen.
- Beleg periodiek in de IB&P jaarplannen het toezicht op het versleutelen, de logging en toegangsdetectie.
- Draag zorg voor vastgestelde selectielijsten en een BiB en vertaal dit naar een bewaar- en vernietigingsbeleid.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Wij hebben de beschreven inrichting (opzet) en operationele uitvoering (bestaan) van de technische en organisatorische beheersingsmaatregelen rondom de verwerking van persoonsgegevens binnen het IMG getoetst. Deze toetsing heeft plaatsgevonden op aandachtsgebieden uit het NOREA Privacy Control Framework (PCF): privacymanagement, gegevensbeveiliging, gebruik, opslaan en verwijderen van persoonsgegevens en het monitoren en handhaven.

Aan de hand van de volgende verwerkingen van persoonsgegevens binnen het IMG, hebben wij de aandachtsgebieden getoetst in opzet en bestaan:

- M10490 Combinatiedossiers versterken en schade
- M10447 Bureau Bijzonder Onderzoek (BBO)
- M10448 Immateriële schade voor kinderen (IMK)
- M10197 Logging en monitoring medewerkers - Immateriële Schade (IMS)
- M9209 Vergoeden van immateriële schade (IMS)

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

4.3 Verspreiding rapport

De opdrachtgever, de heer mr. H.C.D. Korvius, voorzitter van het bestuur van het IMG, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

5 Ondertekening

Den Haag, 1 augustus 2024

Dhr. H.M. van der Beek RO CIPP/E
Projectleider
Auditdienst Rijk

Bijlage 1 – Overzicht hoofdstuk 2

Overzicht hoofdstuk 2
Hieronder is per paragraaf uit het rapport het onderwerp uit het PCF weergegeven dat centraal staat alsmede welke deelvraag het betreft.

Paragraaf	PCF onderwerp	Deelvraag
2.1	1. Privacybeleid 9. Doelbinding 10. Privacyarchitectuur (PbD&D) 18. Beoordeling van compliance met privacywetgeving 19. Periodiek monitoren van privacybeheersingsmaatregelen	1,4
2.2	2. Afbakening van rollen en verantwoordelijkheden 18. Beoordeling van compliance met privacywetgeving 19. Periodiek monitoren van privacybeheersingsmaatregelen	1,4
2.3	3. Identificatie en classificatie van persoonsgegevens 18. Beoordeling van compliance met privacywetgeving 19. Periodiek monitoren van privacybeheersingsmaatregelen	1,4
2.4	7. Competenties medewerkers 8. Bewustwording en training medewerkers	1,2,4
2.5	4. Risicomanagement 5. Data Protection Impact Assesments 18. Beoordeling van compliance met privacywetgeving 19. Periodiek monitoren van privacybeheersingsmaatregelen	1,4
2.6	6. Beheer van privacyincidenten en inbreuken	1,2,4
2.7.1	13. Programma van informatiebeveiliging 18. Beoordeling van compliance met privacywetgeving 19. Periodiek monitoren van privacybeheersingsmaatregelen	1,3,4
2.7.2	14. Identiteit in toegangsbeheer	1,3,4
2.7.3	15. Veilige gegevensoverdracht	1,3,4
2.7.4	16. Versleuteling en eindpuntbeveiliging	1,3,4
2.7.5	17. Registreren van toegang	1,3,4
2.8	11. Bewaren van gegevens 12. Verwijderen, vernietiging en anonimisering	1,4

Bijlage 2 - Managementreactie

Instituut
Mijnbouwschade
Groningen

Retouradres Antwoordnummer 3061, 8000 WB Zwolle

Cascadeplein 10
9726 AD Groningen

Antwoordnummer 3061
8000 WB Zwolle

0800 44 44 111
contact@schadedoormijnbouw.nl

Auditdienst Rijk
Accountdirecteur EZK/LNV
t.a.v. Dhr K.G.M. van den Akker RA
Postbus 20201
2500 EE 's-Gravenhage

Datum 16 mei 2024
Betreft 2024-0000219335 – onderzoeksrapport Bescherming Persoonsgegevens IMG

Referentienummer
IMG/Bestuur/2024/017

Geachte heer Van den Akker,

In onderstaande brief geef ik mijn reactie op het rapport dat door u namens de Auditdienst Rijk (hierna: ADR) aan het Instituut Mijnbouwschade Groningen (hierna: het Instituut) is aangeboden.

1. Achtergrond

In 2023 heeft de ADR een onderzoek gedaan naar de inrichting van de bescherming van persoonsgegevens bij het Instituut. Uit uw onderzoek zijn aanbevelingen gekomen, aan de hand waarvan wij als Instituut onze informatiebeveiliging en privacy huishouding nog verder kunnen professionaliseren. Wij zien uw aanbevelingen als een ondersteuning van het reeds door het Instituut ingezette beleid om privacy en informatiebeveiliging steeds verder te verbeteren. In deze management reactie gaan wij nader in op uw adviezen en op welke wijze het Instituut hier invulling aan geeft.

2. Aanbevelingen en vervolgacties

Naar aanleiding van de aanbevelingen van de ADR heeft het Instituut vervolgacties geformuleerd.

De adviezen van de ADR worden reeds in het jaarplan 2024 meegenomen voor zover daar al geen sprake van was. Mede door de bevindingen van de ADR is reeds gestart met de invulling van een aantal werkzaamheden.

Hieronder volgt per aanbeveling de opvolging door het Instituut.

2.1 Lange termijn operationele borging niet gewaarborgd door tijdelijke medewerkers

De ADR heeft vastgesteld dat veel privacy-gerelateerde rollen en verantwoordelijkheden worden bekleed door (tijdelijke) inhuurkrachten, iets wat volgens de ADR de lange termijn operationele borging van privacy in gevaar brengt. Zij adviseren daarom: *"Maak privacy-gerelateerd wervingsplan en -behoefte onderdeel van het jaarplan om op lange termijn privacy kennis en -expertise te borgen binnen het IMG"*.

Het Instituut kan zich vinden in de aanbeveling om meer medewerkers ambtelijk (vast) in dienst te nemen, met de kanttekening dat het bekleden van alle privacy gerelateerde functies door enkel ambtelijke collega's voor het Instituut op korte termijn niet haalbaar is. Tevens kunnen wij ons vinden in de aanbeveling van de ADR dat deze medewerkers over voldoende kennis en kunde dienen te beschikken. Daarom zal het Instituut bij het werven van nieuwe medewerkers, zoals nu reeds van toepassing, er zorg voor dragen dat deze medewerkers over de juiste competenties beschikken en dat het IMG bij ongeschiktheid alsnog kiest voor tijdelijke expertise van buiten. Uiteraard herkent het IMG dat de kennisborging van essentieel belang is en wordt dit in de wervingsparagraaf van het IB&P beleid uitgewerkt.

2.2 Bijzondere persoonsgegevens

De ADR benoemt dat richtlijnen omtrent de verwerking van bijzondere persoonsgegevens niet vastliggen. De ADR beveelt daarom aan: *"Beschrijf in het privacy beleid aanvullende uitgangspunten en uitzonderingsgronden om bijzondere categorieën van persoonsgegevens te mogen verwerken. Besteed hierbij tevens aandacht aan noodzakelijke technische en organisatorische maatregelen die deze verwerking mogelijk kunnen maken."*

Het Instituut is bij de verwerking van bijzondere persoonsgegevens gebonden aan de wet. De wet geeft dan ook de richtlijnen waaraan het Instituut zich moet houden bij de verwerking van bijzondere persoonsgegevens. Het is daarom niet noodzakelijk hier apart beleid voor te ontwikkelen. Het Instituut beziet steeds per regeling wat de wettelijke grondslag voor de verwerking is. Evenwel ziet het IMG toegevoegde waarde om in het IB&P beleid wel een paragraaf op te nemen die deze werkwijze expliciet maakt. In het privacy beleid zal dit worden opgenomen in de tekst. De afgelopen jaren zijn extra beleidsparagrafen geschreven op basis van ontwikkelingen binnen het Instituut. Deze zijn tot nu toe in aparte documenten opgenomen. In 2024 zullen deze aanpassingen integraal opgenomen worden in het beleid. Hiermee geven we tevens gehoor aan de aanbeveling *"Herzie het privacy beleid en besteed hierbij expliciet aandacht aan uitgangspunten rondom privacy by design/default alsmede de controle hierop"*.

2.3 Datalekken

De ADR doet een aanbeveling die ziet op het uitbreiden van het datalekkenregister, namelijk: *"Breid het register van datalekken uit met datum en tijd melding AP en/of betrokkenen alsmede benodigde bijlages om controle op basis van het register mogelijk te maken"*.

Het Instituut neemt deze aanbeveling over. De aanbevolen wijzigingen gaat het Instituut doorvoeren in het register.

2.4 Monitoren en toezicht

De ADR doet drie aanbevelingen inzake de monitoring van, en het toezicht op, de privacy(risico's). Deze aanbevelingen van de ADR zijn: *"Draag zorg voor voldoende capaciteit en aandacht om controle en monitoringsactiviteiten uit de derde lijn te laten uitvoeren", "Beschrijf criteria op basis waarvan privacy risico's worden vastgesteld, geaccepteerd en gedocumenteerd" en "Besteed extra aandacht aan het monitoren en toezichthouden op de uitvoering van de uit de DPIA voortgekomen noodzakelijk technische en organisatorische maatregelen."*

Het instituut herkent deze aanbevelingen en ziet dit als ondersteuning van het reeds ingezette beleid voor 2024. In samenwerking met de afdeling Interne Controle wordt een procedure voor controle op DPIA maatregelen ingericht op basis waarvan de afdeling Interne Controle in samenwerking met de Functionaris Gegevensbescherming monitort en toeziet op de opvolging van maatregelen.

2.5 Terugkerende taken

De ADR stelt daarnaast een aantal aanbevelingen die betrekking hebben op de jaarlijks terugkerende taken van het privacy team. Een jaarlijks terugkerend punt in het privacy jaarplan is het uitvoeren van DPIA's. Voor 2024 staan veel DPIA's op de planning. Aan de hand van de uitgevoerde DPIA's wordt ook het verwerkingsregister verder aangevuld. Ook processen waarop geen DPIA hoeft te worden uitgevoerd, maar waarin wel persoonsgegevens worden verwerkt, worden dit jaar opgenomen in het verwerkingsregister. De aanbevelingen *"Realiseer het voornemen om het register van verwerkingsactiviteiten voor de uitvoeringen van regelingen verder te vullen om uiteindelijk controle en monitoring op basis van het register te kunnen bewerkstelligen"* en *"Realiseer het voornemen om de resterende DPIA's op korte termijn af te ronden"* worden in deze planning mee genomen.

Het Instituut heeft de DPIA's op de planning staan voor 2024. Daarnaast staat ook op de planning voor 2024 om zo de verwerkingen binnen het Instituut aan te vullen in het register.

Zowel in het Informatiebeveiliging als Privacy jaarplan wordt aansluiting gezocht bij de plannen en ontwikkelingen binnen het Instituut. Zo kan er voor alle domeinen binnen het Instituut ingespeeld worden op de vragen die er spelen, en kan het IB&P team ondersteunen waar nodig. Ook is er aandacht voor awareness in deze jaarplannen. De aanbeveling *"Maak bewustwordingsactiviteiten verplicht zodat iedere medewerker aantoonbaar groeit op het gebied van privacy en gegevensbescherming"* neemt het Instituut dan ook mee in de plannen voor dit jaar.

2.6 Informatiebeveiliging

De ADR geeft ook een aantal aanbevelingen op het gebied van informatiebeveiliging. De aanbeveling *"Beschrijf en koppel aan de diverse beleidstukken welke privacy-specifieke technische en organisatorische maatregelen genomen (dienen te) worden"* zal door het Instituut worden opgepakt. De tweede aanbeveling betreft: *"Stel procedures op, op basis van vastgesteld beleid, voor het versleutelen van gegevens, logging en voor toegangsdetectie en monitoringssystemen"*.

Het Instituut neemt voor alle kern-applicaties diensten af van de interne ICT dienstverleners van het ministerie van economische zaken (DICTU), van de Rijksdienst Voor Ondernemend Nederland (RVO) en van de externe leverancier van de deskundigentool. De eerste twee leveranciers voldoen

zelfstandig aan de informatiebeveiligingseisen en verantwoorden dat zelfstandig aan de eigenaar binnen EZK. Voor wat betreft de deskundigentool, zijn de eisen voor Informatiebeveiliging in het contract opgenomen en maakt de verantwoording onderdeel uit van de ISO 270001 certificering van de leverancier. Daarnaast merkt het Instituut op dat het versleutelen van data geschiedt volgens het "Jericho" principe. Dit principe houdt kort gezegd in dat de data beveiligd wordt in elke omgeving en object waar het zich bevindt. Materieel gezien is de beveiliging van persoonsgegevens hierdoor geborgd. De aanbeveling van de ADR wordt door het Instituut dan ook ingevuld door extra aandacht voor het toezien op de maatregelen. Het Instituut onderneemt de noodzakelijke acties om er zorg voor te dragen dat zij ook daadwerkelijk de stukken in het bezit heeft om aan te tonen. Eveneens zal het Instituut dit opnemen in het Informatiebeveiliging en Privacy beleid.

De laatste aanbeveling van de ADR op het gebied van informatiebeveiliging neemt het Instituut eveneens over. Het toezicht op het versleutelen, loggen en toegangsdetectie zal worden opgenomen in de jaarplannen van het IB&P team.

Ik wil de ADR bedanken voor haar uitgebreide rapport en aanbevelingen. Wij zien dit als een goede ondersteuning voor het reeds door ons ingezette beleid.

Met vriendelijke groet,

Mr. H.C.D. (Henk) Korvinus
Voorzitter Bestuur Instituut Mijnbouwschade Groningen

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00