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