

Van het kopiëren en gebruik van productiedata behoort verslaglegging te worden bijgehouden om in een audittraject te voorzien. Het verslag dient tenminste te bevatten:

- Omschrijving van de gebruikte dataset;
- Datum en tijdstip kopieeractie data naar de acceptatieomgeving;
- Resultaat integriteitscontrole;
- Datum en tijdstip verwijdering data uit de acceptatieomgeving.
- Datum en tijdstip verwijdering van gegevens bij externe partijen.

Logging en monitoring moeten conform het beleid van het Intituut¹¹ worden ingericht, zodat bij incidenten de impact beter ingeschat kan worden.

4.3 Risico-acceptatie

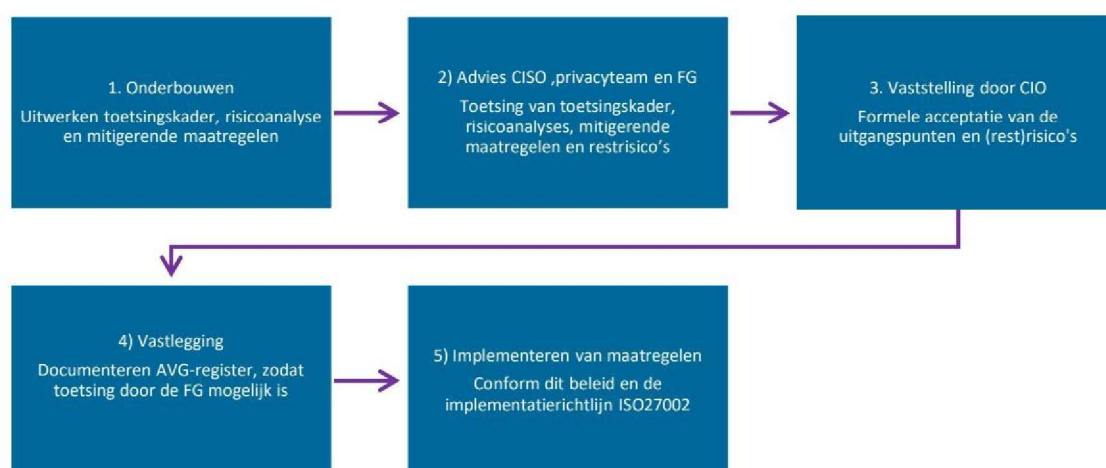
Indien blijkt dat na het mitigeren van de risico's er nog steeds een (aanzienlijk) risico bestaat voor de bescherming van de persoonlijke levenssfeer van de betrokkene, dan kan het projectteam/ de tester ervoor kiezen om de test doorgang te laten vinden. Het projectteam / de tester mag dit alleen doen, indien hij gemotiveerd kan toelichten waarom de test noodzakelijk is en de test een ander zwaarwegender belang dient dat eveneens in voordeel is van de betrokkene. Hiervoor dient het projectteam/ de tester samen met de CIO een risico-acceptatie te ondertekenen, die opgesteld wordt door het team IB&P. In die risico-acceptatie worden mitigerende maatregelen / oplossingen vastgelegd om naleving van de AVG op een korte termijn te bewerkstelligen. Tevens zal er in deze risico-acceptatie monitoring en toezicht afspraken worden vastgelegd, waarbij IB&P gevraagd inzage kan krijgen in de voortgang van het projectteam / de tester om de test AVG compliant te laten worden. **Let op:** dit kan alleen voor testen worden gedaan die na het nemen van maatregelen geen hoog risico's meer bevatten in de zin van artikel 35 en 36 AVG. Testen die na het nemen van hoog risico's bevatten moeten namelijk volgens de AVG worden voorgelegd aan de Autoriteit Persoonsgegevens.

¹¹ S. Dollen, 'Logging en monitoringsbeleid Instituut Mijnbouwschade Groningen (IMG),' versie 1, 22 juli 2021.

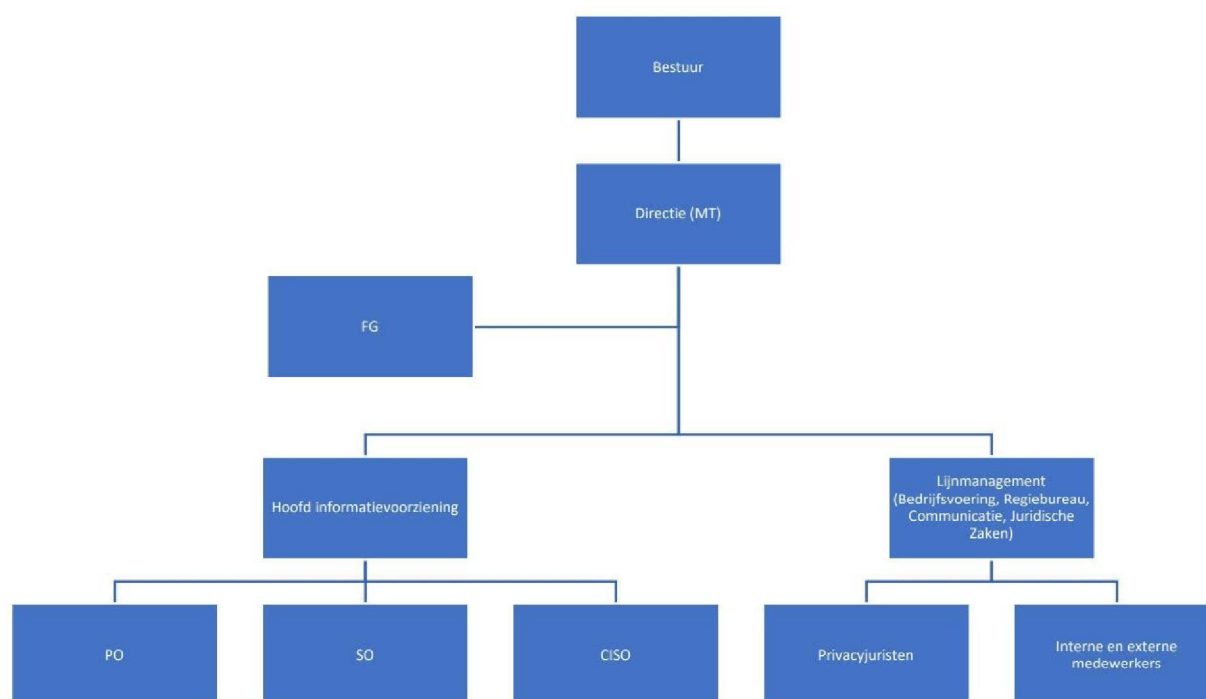
5 Procedure

Om te mogen testen met productiedata dient de volgende procedure te worden gevolgd. De uitwerking van bovenstaand toetsingskader en de risicoanalyse moet worden gedocumenteerd en akkoord bevonden door de CIO na een positief advies van de CISO, het privacyteam en de Functionaris Gegevensbescherming (hierna: FG). Het projectteam is verantwoordelijk voor het uitwerken van dit toetsingskader en wordt zo goed mogelijk ondersteund door IB&P bij deze uitwerking. De onderbouwing bevat naast de risicoanalyse een beschrijving van welke mitigerende maatregelen worden voorgesteld. Op basis van de adviezen van IB&P kan het projectteam beslissen over te nemen maatregelen en om de eventuele (rest) risico's formeel accepteren met de CIO. Indien het risicoprofiel van de applicatie die wordt getest dermate hoog of politiek-bestuurlijk gevoelig ligt wordt er een formeel advies van de FG gevraagd. Blijven de risico's dermate hoog en zijn deze niet te mitigeren, dan dient de Autoriteit Persoonsgegevens geraadpleegd te worden.

5.1 Procedure schematisch weergegeven



Schematisch gezien zien de interne rollen ten opzichte van elkaar er als volgt uit:



Bijlage I: Stroomschema testen met persoonsgegevens



Beleid Privacy by Design & Privacy by Default
Instituut Mijnbouwschade Groningen (het
Instituut)

Versie 1.0

Datum	december 2024
Status	Definitief

Colofon

Projectnaam

Contact

Beleid Privacy by Design & Privacy by Default

5.1.2e

pschadedoormijnbouw.nl

Auteurs

5.1.2e

Versie

Bijlage(n)

1.0

0

Versie	Datum	Status	Toelichting
0.1	10 september 2024	Concept	Opstelling document
0.2	17 oktober 2024	Concept	Verwerken feedback
0.3	1 november 2024	Concept	Feedback verwerkt
1.0	10 december 2024	Definitief	Vastgesteld

Inhoudsopgave

Colofon—2

1	Aanleiding—4
2	Inleiding—4
2.1	Definities—5
2.2	Toepassingsgebied—5
2.3	Verantwoordelijkheid— Fout! Bladwijzer niet gedefinieerd.
2.4	Belang van Privacy by Design— Fout! Bladwijzer niet gedefinieerd.
2.5	Voorwaarden borging van Privacy by Design—6
2.6	Opbouw van het beleidskader Privacy by Design—6
3	Kaders—7
3.1	Eisen AVG—7
3.2	Principes Privacy by Design—7
4	Inrichting Privacy by Design—9
4.1	Procesfases bij de ontwikkeling van een product of dienst—9
4.2	Verantwoordelijkheden—11
5	Technische en organisatorische maatregelen—13
5.1	Privacy by Design Strategies—13

1 Aanleiding

Bescherming van persoonsgegevens is in onze digitale samenleving een belangrijk aandachtspunt. De Algemene verordening persoonsgegevens (hierna: AVG) geeft hier handvatten voor. Deze verordening geeft de beginselen weer waaraan verwerking van persoonsgegevens moet voldoen, benoemt de juridische grondslagen waarop gegevensverwerking kan worden gebaseerd en geeft de rechten waar betrokkenen van wie persoonsgegevens worden verwerkt zich op kunnen beroepen. In artikel 25 van de AVG staat het beginsel van Privacy by Design en Privacy by Default waar bij de verwerking van persoonsgegevens aan moet worden voldaan. Hierbij dient rekening gehouden te worden met het beschermen van persoonsgegevens door middel van het nemen van passende technische en organisatorische maatregelen.

Voor het Instituut Mijnbouwschade Groningen (hierna: het Instituut) betekent dit dat de beginselen van gegevensbescherming door ontwerp (Privacy by Design) en de standaardinstellingen (Privacy by Default) moeten worden toegepast. Het is belangrijk dat de uitgangspunten van zowel Privacy by Design als Privacy by Default gedurende het hele proces van gegevensverwerking in acht worden genomen. Dit is bijvoorbeeld bij het ontwikkelen van de systemen waarin de gegevens worden verwerkt tot het moment dat deze gegevens definitief worden verwijderd. Maar ook bij de al draaiende projecten en systemen moeten de beginselen in acht worden genomen en moet worden getoetst of hieraan voldaan is.

Zoals eerder aangegeven komt Privacy by Design (hierna: PbD) voort uit de AVG. De vroegtijdige implementatie van PbD kan financiële voordelen opleveren, doordat minder gegevens worden verwerkt en niet achteraf aanpassingen hoeven te worden gedaan aan een al ontwikkeld systeem of product. Het consequent toepassen van PbD levert echter vooral waarde op in de vorm van een betere bescherming van de privacy van betrokkenen. Dit sluit aan bij het centrale uitgangspunt van het Instituut als het gaat om gegevensverwerking: 'Bij het Instituut Mijnbouwschade Groningen zijn uw gegevens in goede handen'.

De Ministeries van Economische Zaken en Klimaat (EZK) en Landbouw, Natuur en Voedselklimaat (LNV) hebben voor PbD gezamenlijk een beleidskader opgesteld waaraan al hun kerndepartementen en andere organisatieonderdelen zich moeten houden. Zelfstandige bestuursorganen, waaronder het Instituut, vallen buiten de scope van het beleidskader van EZK en LNV. Het voorliggende beleid is specifiek voor en door het Instituut opgesteld, maar is op een aantal punten gebaseerd op het beleid van EZK en LNV. Dit wordt ook aangemoedigd door het EZK en LNV.¹

¹ Paragraaf 2.1.2 Beleidskader Privacy by Design EZK en LNV.

2

Inleiding

2.1

Definities

AVG	Algemene Verordening Gegevensbescherming
Betrokkene	Een natuurlijk persoon over wie de persoonsgegevens gaan. Bij het Instituut zijn de betrokkenen in de meeste gevallen aanvragers van schaderegelingen en medewerkers van het Instituut
EZK	Ministerie van Economische Zaken en Klimaat
Het Instituut	Instituut Mijnbouwschade Groningen
PbD	Privacy by Design & Privacy by Default
Persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Systeem of Dienst	Waar het gaat om Systemen kan bedoeld worden op systemen die door het Instituut zelf zijn ontwikkeld of door derde partijen. De diensten van het Instituut zien op de afhandeling van schade.

2.2

Toepassingsgebied

Dit beleid is van toepassing op alle processen waarin persoonsgegevens worden verwerkt binnen het Instituut. Hierbij is in het bijzonder aandacht voor de ontwikkeling van nieuwe of gewijzigde processen omdat Privacy by Design en Default hierin nog makkelijk geïmplementeerd kunnen worden. Bij elke fase van de ontwikkeling en uitvoering van een nieuwe dienst of een nieuw systeem, product of proces dient echter rekening te worden gehouden met privacy en de uitgangspunten van PbD. Hierbij zullen onder andere de standaardinstellingen bij elke fase van de dienst of het product zo moeten worden ingesteld dat de privacy van betrokkenen zo goed mogelijk gewaarborgd wordt. Dit begint bij het ontwerp en eindigt bij de oplevering. Daarnaast is ook het periodiek reviewen van de privacywaarborgen bij de verwerkingen van belang. Wanneer het Instituut constateert dat een systeem geoptimaliseerd kan worden op het gebied van privacy dan worden de benodigde acties uitgezet.

2.3

Verantwoordelijkheden

Dit PbD-beleid is op alle afdelingen en verwerkingen van het Instituut van toepassing. Daarnaast is het belangrijk dat deze beginselen ook in acht worden genomen door derde partijen die namens het Instituut producten of diensten ontwikkelen en gegevens verwerken. De kaders die dit beleid geeft kunnen verder afgestemd worden op specifieke verwerkingen. Wanneer er vragen zijn over het PbD-beleid in het algemeen, of voor specifieke verwerkingen, kunnen deze worden voorgelegd aan het privacyteam (via privacy@schadedoormijnbouw.nl). Zij kunnen adviseren over het implementeren van deze beginselen.

2.4 Belang van Privacy by Design

De AVG eist dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen neemt bij het ontwerpen of ontwikkelen van nieuwe diensten of producten die persoonsgegevens verwerken.² Bij elke fase van de ontwikkeling moet worden nagedacht over hoe persoonsgegevens het beste kunnen worden verwerkt en beschermd. Hierdoor zullen de beginselen uit de AVG, zoals het beginsel van dataminimalisatie, doeltreffender worden nageleefd. Door al voor de ontwikkeling van een nieuw product of nieuwe dienst na te denken over de implementatie van de beginselen uit de AVG kunnen kosten worden bespaard, omdat niet achteraf nog wijzigingen hoeven te worden doorgevoerd in een (complex) systeem. Het grootste voordeel van de toepassing van PbD zit hem echter in de betere bescherming van persoonsgegevens van betrokkenen. Zo kan er bijvoorbeeld worden besloten om bepaalde gegevens niet te verwerken omdat deze niet noodzakelijk zijn voor de verwerking. Ook kunnen de persoonsgegevens die verwerkt worden geanonimiseerd of gepseudonimiseerd worden. Het risico op datalekken kan door PbD verkleind worden omdat risico's bij de ontwerpfase al gesignaleerd zijn. Waar mogelijk kunnen voorafgaand aan de verwerking dan al maatregelen genomen worden om risico's te beperken. Ten slotte heeft PbD een positief effect op compliance en accountability omdat medewerkers worden aangemoedigd na te denken over eventuele risico's en maatregelen. PbD zorgt ervoor dat het Instituut zich gedurende het hele proces bewust is van de verwerkingen en de risico's en zo de benodigde maatregelen kan nemen.

2.5 Voorwaarden borging van Privacy by Design

Om PbD succesvol uit te voeren bij het Instituut, is er bewustzijn bij de medewerkers nodig. Zij moeten bij de ontwikkeling van elke nieuwe dienst of product nadenken over de waarborging van de privacy van betrokkenen. De medewerkers moeten in staat zijn om privacy risico's te signaleren en waar nodig passende technische en organisatorische maatregelen te nemen om de gegevensbescherming zo goed mogelijk te waarborgen. Om dit te realiseren moet het Instituut ervoor zorgen dat medewerkers de hiervoor de benodigde kennis hebben.

2.6 Opbouw van het beleid Privacy by Design

In dit beleid zal eerst worden ingegaan op de eisen voor succesvolle toepassing van PbD uit de AVG. Hierbij zijn, zoals ook in het beleid van EZK en LNV, de zeven basis principes van Ann Cavoukian voor het implementeren van PbD leidend.³ Daarna wordt uitgewerkt hoe PbD wordt toegepast in de processtromen van de organisatie van het Instituut. Ten slotte zal worden stilgestaan bij het inbedden van PbD dat door middel van technische en organisatorische maatregelen gebeurt.

² Zie art. 25 AVG.

³ https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

3 Kaders

3.1 Eisen uit de AVG

In artikel 25 van de AVG besteedt de wetgever aandacht aan Privacy by Design en Privacy by Default. Dit artikel bepaalt dat de verwerkingsverantwoordelijke doeltreffend uitvoering geeft aan de principes voor gegevensbescherming bij zowel het bepalen van de verwerkingsmiddelen als het uitvoeren van de verwerking zelf. Daarbij is de toepassing van PbD een essentieel onderdeel. PbD bestaat volgens de AVG uit het nemen van organisatorische maatregelen, waar bijvoorbeeld de primaire processtromen met privacy in gedacht worden ingericht.

Voorts bestaat PbD uit het nemen van technische maatregelen. Deze maatregelen zijn technologieën die gemaakt zijn met de huidige stand van de techniek (zie [Hoofdstuk 5](#) voor meer informatie). Privacy by Default ziet op de standaardinstellingen die gekozen worden: ook hier moet privacy de hoofdrol spelen, en moeten de standaardinstellingen zo privacy vriendelijk mogelijk zijn. Tot slot dient hier een risico gerichte aanpak gebruikt te worden, waarbij de producten of diensten conform de privacycriteria worden ingericht.

3.2 Principes Privacy by Design en de invulling van deze principes door het Instituut

De term Privacy by Design is ontwikkeld door Ann Cavoukian in de jaren 90. Volgens haar kan de term onderverdeeld worden in 7 principes. Deze principes zijn hieronder beschreven en kunnen onder andere worden toegepast op applicaties, digitale infrastructuur en informatiehuishoudens. Op een aantal punten zijn de principes aangepast of aangevuld om ervoor te zorgen dat deze op een heldere en praktische wijze kunnen worden toegepast bij het Instituut.

1. *PbD is een proactieve benadering.*

PbD wordt toegepast om vooraf na te denken over privacyrisico's en deze risico's te verkleinen door het vooraf implementeren van maatregelen (*'Proactive not Reactive; Preventative not Remedial'*).⁴ Dit betekent dat mensen moeten gaan nadenken over de privacyaspecten van hun werk, en hoe dit betrokkenen raakt. Voor het Instituut betekent dit dat al bij de gesprekken over het implementeren van nieuwe systemen, of het aangaan van nieuwe samenwerkingen wordt gekeken naar de eventuele privacy risico's. Ook gedurende deze processen moeten eventuele privacy risico's in acht worden genomen. Bestaande verwerkingsprocessen moeten periodiek getoetst worden om ervoor te zorgen dat de privacy van betrokkenen gewaarborgd blijft. Het privacy-team kan de desbetreffende afdelingen hierin bijstaan. Ook wanneer een middel als een Data Protection Impact Assessment (DPIA) niet nodig is om risico's in kaart te brengen, kan door adviesvragen extra aandacht worden besteed aan eventuele privacy risico's.

2. *Privacy by Default, gegevensbescherming als standaardinstelling, is de regel.*

Privacy by Default streeft naar een maximaal niveau van privacy door te verzekeren dat persoonsgegevens automatisch beschermd zijn in alle systemen en overige processen, zonder dat de betrokkene daar zelf een handeling voor hoeft te verrichten. Hierbij zijn de standaardinstellingen van een product of dienst op het maximale niveau qua gegevensbescherming ingesteld. Bij deze standaardinstelling zal gedacht moeten worden aan de volgende standaarden:

- Verwerken van persoonsgegevens op een passende wijze: Dit houdt in dat de persoonsgegevens op een rechtmatige, behoorlijke en transparante manier

⁴ Principe 1 van Privacy by Design door Ann Cavoukian.

voor een welbepaald, uitdrukkelijk en gerechtvaardigd doeleinde verwerkt worden.

- Het beginsel van dataminimalisatie wordt in acht genomen: Enkel de persoonsgegevens die noodzakelijk zijn voor het doeleinde worden verwerkt.
- Openbaarmaking van persoonsgegevens: De openbaarmaking van persoonsgegevens moet beperkt worden tot degene aan wie de persoonsgegevens horen, ofwel de betrokkene.
- Bewaartermijnen van persoonsgegevens: Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij verwerkt zijn.
- Verwerken van privacy verzoeken: Het Instituut moet kunnen aantonen in hoeverre verzoeken en klachten gerelateerd aan privacy worden afgehandeld binnen de organisatie.

Inachtneming van deze standaarden zorgt ervoor dat de privacy van betrokkenen beter beschermd is, omdat privacy overal in het proces wordt meegenomen. Over de inachtneming van deze maatregelen is ook in de externe privacyverklaring informatie opgenomen (bijvoorbeeld over bewaartermijnen en welke gegevens worden verwerkt).

3. *PbD moet verankerd zijn in het ontwerp*

Bij alle (mogelijke) verwerkingen die het Instituut van plan is uit te voeren of al uitvoert, moeten medewerkers nadenken over PbD. Dit kan door zelf bewust na te denken over de principes, bijvoorbeeld aan de hand van het voorliggende beleid, of door adviesvragen te stellen aan de medewerkers van het team informatiebeveiliging en privacy.

De manier waarop privacy in acht is genomen tijdens het ontwerp moet daarnaast worden vastgelegd zodat de overwegingen kunnen worden getoetst.. Overwegingen die gebruikt zijn bij het ontwerpen kunnen belangrijke inzichten geven en maken keuzes en overwegingen achteraf re-construeerbaar. Hierdoor kan het proces goed geëvalueerd worden.

4. *Privacy mag niet ten koste gaan van andere rechten en waarborgen, en wordt door alle medewerkers in acht genomen*

Het toepassen van privacy zorgt er niet voor dat op andere vlakken wordt gecompenseerd, om betere bescherming van privacy mogelijk te maken. Betere bescherming van privacy mag echter niet ten koste gaan van andere rechten en waarborgen voor betrokkenen. Het recht op een veilige leefomgeving voor de Groningers en Drentenaren mag bijvoorbeeld niet in het geding komen doordat de privacybeschermingsmaatregelen te restrictief werken. .

5. *PbD pas je toe gedurende de gehele levenscyclus van een persoonsgegeven.*

PbD richt zich in eerste instantie vooral op de ontwerpfase. Het waarborgen van privacy duurt echter de gehele levenscyclus van een verwerking.

- Tijdens het bedenken (ontwerpfase: doel bepalen);
- vervolgens tijdens het vormgeven en ontwikkelen van de verwerking (uitvoering bepalen/implementatie);
- het daadwerkelijk uitvoeren van de verwerkingen (beheer);
- het uiteindelijke afronden van de verwerking wat kan bestaan uit het archiveren of het vernietigen van de persoonsgegevens.

Het is daarom van belang dat medewerkers worden meegenomen in de overwegingen achter bepaalde privacykeuzes, zodat zij zich bewust zijn van het belang van PbD.

6. *Zichtbaarheid en transparantie*

Binnen het Instituut wordt PbD geïmplementeerd op een wijze die voor alle belanghebbenden waarborgt dat alle privacy gerelateerde discussies, beoordelingen en besluiten transparant en zichtbaar zijn. Dit betekent dat uit de documentatie voor nieuwe diensten of producten moet blijken dat de PbD processtappen van hoofdstuk 4 zijn doorlopen. Uit deze documentatie moet ook blijken waarom bepaalde keuzes zijn gemaakt en hoe deze beslissingen bijdragen aan de bescherming van persoonsgegevens.

Voor dit principe zijn een aantal uitgangspunten uit de AVG extra van belang. Door een duidelijk en transparant privacybeleid (waar Privacy by Design en Default onderdeel van uitmaken) kan het Instituut laten zien dat hij verantwoordelijk omgaat met persoonsgegevens, en de betrokkene hierin voorop stellen. Dit is binnen het Instituut onder andere gewaarborgd door persoonsgegevens alleen te verwerken als dit op een verantwoorde manier kan, waarbij voorzienbaarheid voor de burger in mee wordt genomen.

7. *Het belang van de betrokkene staat centraal*

Het doel van PbD is pas bereikt als de rechten en vrijheden van betrokkenen op het gebied van persoonsgegevens in alle fases van het proces daadwerkelijk zijn beschermd. Het doel van de AVG is dat betrokkenen meer controle krijgen over hun eigen gegevens. Het Instituut en zijn organisatieonderdelen streeft naar maximale transparantie en open communicatie met de burgers en houdt rekening met de impact die de verwerking kan hebben op de burger.

Hierbij staan een aantal uitgangspunten uit de AVG in het bijzonder centraal:

- Betrokkenen hebben recht op toegang tot de gegevens die van hen verwerkt worden. Hierdoor hebben zij zelf controle over hun persoonsgegevens.
- Waar nodig wordt om toestemming voor de verwerking gevraagd.
- Betrokkenen worden voorgelicht over de verwerkingen die plaats vinden. De privacyverklaring wordt regelmatig gecontroleerd en geüpdatet en waar nodig worden betrokkenen tijdens het proces voorgelicht over specifieke verwerkingen.

4 Inrichting Privacy by Design en Default

4.1 Fases bij de ontwikkeling van een systeem of dienst

4.1.1 *Inrichting PbD*

Dit hoofdstuk bevat de verschillende fases waar je bij de ontwikkeling van een dienst of systeem dat persoonsgegevens verwerkt doorheen kan gaan. In deze procesbeschrijving wordt duidelijk gemaakt op welke manier PbD kan worden betrokken bij de ontwikkeling van nieuwe producten of diensten. De fases zullen niet altijd duidelijke kaders hebben, in sommige gevallen lopen deze in elkaar over. De fases worden hieronder verder uitgewerkt, waarbij er per fase is aangegeven hoe Privacy by Design en Default in deze fase een rol kunnen spelen. PbD moet gedurende de hele verwerking worden toegepast, en stopt dus niet na de ontwikkeling. Deze stappen zouden bij elke ontwikkeling van nieuwe systemen of diensten moeten worden doorlopen.

Ontwerp: het ontwerp bestaat uit het bepalen van doelen en de invulling van de verwerking. Bij het bepalen van het doel wordt eerst onderzocht of persoonsgegevens echt nodig zijn om het doel te kunnen bereiken. In deze fase wordt ook gekeken welke technische en organisatorische maatregelen nodig zijn.

Implementatie: implementatie ziet op het realiseren van het ontwerp of het laten uitvoeren door een externe partij. Het in praktijk brengen van het verwerkingsproces in de vorm van het aanpassen of invoeren van een systeem.

Uitvoering: het beheren van het goedgekeurde systeem en het daarbij behorende verwerkingsproces.

Bijstellen of afbouwen: het aanpassen of beëindigen van het proces en het eventueel verwijderen of archiveren van de gegevens.

4.1.2 *Ontwerp*

In de ontwerpfase moeten de volgende punten in acht worden genomen:

- **Doel vaststellen:** de verantwoordelijke stelt vast wat het onderliggende doel van de dienst of het product is.
- **Noodzaak bepalen:** vaststellen wat nodig is om het doel te kunnen behalen. Hierbij staat de noodzaak om persoonsgegevens te gebruiken centraal. Daarnaast zal er gekeken moeten worden wat de relatie is tussen het te bereiken doel en de persoonsgegevens.
- **Toetsen aan rechtmatigheid:** hierbij wordt gekeken naar de grondslag voor het gebruik van de persoonsgegevens. Deze grondslagen zijn opgenomen in de AVG.⁵ Voor het Instituut kan de grondslag voor de gegevensverwerking voornamelijk in de Tijdelijke wet Groningen worden gevonden.
- **Dataminimalisatie en overige waarborgen:** vervolgens wordt bepaald welke persoonsgegevens noodzakelijk zijn om het doel te bereiken. Op welke manier worden de persoonsgegevens verzameld, op basis van welke grondslag worden bepaalde categorieën persoonsgegevens verwerkt, hoelang mogen de gegevens worden bewaard, zijn de persoonsgegevens nog accuraat, zijn de gegevens rechtmatig verkregen en is de betrokkene op de hoogte dat diens persoonsgegevens verwerkt worden.

Deze punten worden, in samenspraak met het privacyteam, bij het opstarten van een project beoordeeld. Hierdoor kunnen bij aanvang van een project direct de

⁵ Zie art. 6 AVG.

juiste keuzes worden gemaakt waar het gaat om de inrichting van een systeem. Voor elk project wordt er een "Project Start Architectuur" (PSA) opgemaakt, waarin staat opgenomen dat een projecteigenaar langs het privacyteam dient te gaan om het project te laten toetsen op o.a. PbD beginselen. Deze vragen die in de ontwerpfase moeten worden beantwoord zullen ook terugkomen in de DPIA, indien het privacyteam oordeelt dat een DPIA nodig is. Wanneer geen DPIA nodig is zullen deze vragen in een memo voor het project opgenomen worden en worden aangehecht aan de PSA.

4.1.3 *Implementatiefase*

Bij de implementatie wordt gekeken hoe een systeem of werkwijze op een zo privacy vriendelijke manier ingezet kan worden door het Instituut. Dit is ook van belang wanneer een systeem is ingekocht door het Instituut. In de implementatiefase is het van belang dat het privacyteam op tijd wordt bijgeschakeld, zodat de toetsing van de PbD beginselen in de ontwerpfase wederom kunnen worden getoetst bij de implementatiefase. Daarmee kan worden getoetst of de afspraken die zijn gemaakt in de ontwerpfase met betrekking tot PbD beginselen gerealiseerd zijn voordat het project wordt geïmplementeerd. Ook bestaat er in deze fase de mogelijkheid om wederom te toetsen of een impact assessment (DPIA/DPIA licht) noodzakelijk is..

4.1.4 *Uitvoeringsfase*

De uitvoeringsfase is de fase waarin een systeem daadwerkelijk ingezet wordt door het Instituut voor de verwerking waarvoor dit systeem ontwikkeld is. In deze fase moet periodiek worden geëvalueerd of de gegevensverwerking conform de beginselen van PbD gebruikt wordt. Bij oplevering van een systeem wordt deze toetsing uitgevoerd in een DPIA. Door een DPIA periodiek te herzien wordt voorzien in een systeem van monitoring van de PbD beginselen. Door PbD goed toe te passen zorgt het Instituut ervoor dat enkel de gegevens die noodzakelijk zijn op een juiste manier worden verwerkt.

4.1.5 *Afbouwfase*

De afbouwfase begint wanneer een systeem of product niet langer gebruikt wordt. Hiervoor moeten projectteams een afbouwplan volgen. In dit afbouwplan is aandacht voor de bewaartermijnen van gegevens, maar ook het beschikbaar houden van gegevens als een systeem wordt afgebouwd wanneer de bewaartermijn van de gegevens nog niet is verstreken. In deze fase speelt PbD een rol bij het juist toepassen van bewaartermijnen om ervoor te zorgen dat gegevens niet langer worden bewaard dan nodig is.

4.2 **Verantwoordelijkheden**

Het uiteindelijke doel van het PbD-beleid is dat het Instituut gegevens op een zo privacy vriendelijk mogelijke manier verwerkt. Medewerkers moeten in staat zijn om PbD toe te passen en moeten er voor zorgen dat zij producten en diensten opleveren die voldoen aan de privacycriteria. Naast het afdwingen van het zorgvuldig omgaan met persoonsgegevens, kan PbD ook bijdragen aan het verminderen van het gebruik van persoonsgegevens. Om dit zo effectief mogelijk te doen ligt het zwaartepunt van PbD vooral in het begin van het proces.

De verantwoordelijkheid voor het voldoen aan PbD beginselen ligt bij de projectleider.⁶ Deze is verantwoordelijk voor het tijdig aanhaken van het Privacyteam en het op tijd aanleveren van informatie wanneer hierom gevraagd wordt.

⁶ Zie hoofdstuk 4 van het herziene privacybeleid IMG.

Binnen het Instituut is het team Informatiebeveiliging en Privacy gespecialiseerd in het beoordelen van gegevensverwerkingen in nieuwe processen. Wanneer er voornemens zijn om nieuwe processen te ontwikkelen waarin persoonsgegevens worden verwerkt dan moet het Privacyteam hierbij worden aangehaakt. Zo zorgen we ervoor dat er waarborgen worden ingebouwd om de privacyrechten van betrokkenen te beschermen en ervoor te zorgen dat een proces zo privacyvriendelijk mogelijk is ingericht. Projectteams die zich bezighouden met het uitwerken van nieuwe ideeën moeten daarom zo vroeg mogelijk in het proces ervoor zorgen dat zij team Informatiebeveiliging & Privacy benaderen voor advies over de voorgenumen verwerking.

Om hier een eenduidige procedure voor op te stellen wordt dit beleid versterkt door een werkinstructie, die later als bijlage bij dit beleid zal worden gevoegd. Deze werkwijze geeft de verschillende afdelingen die zich bezig houden met gegevensverwerking een praktische handleiding om er zo voor te zorgen dat PbD zo breed mogelijk door de organisatie wordt gevolgd.

4.3

Inrichten Privacy by Default

Bij het inrichten van processen met inachtneming van de beginselen van Privacy by Default gaat het om het kiezen van de meest gunstige privacyinstellingen voor de betrokkenen. Hierbij moet onder andere worden gekeken naar welke gegevens nodig zijn met het oog op doelbinding en de minimale gegevensverwerking. Om Privacy by Default zo optimaal mogelijk door te voeren moet het Instituut ervoor zorgen dat aanvragers enkel de gegevens doorgeven en hoeven door te geven die nodig zijn voor hun aanvraag. Vervolgens moet het Instituut ervoor zorgen dat binnen het Instituut ook enkel de gegevens die nodig zijn worden verwerkt. Dit is door het Instituut te realiseren door enkel die gegevens uit te vragen die daadwerkelijk nodig zijn voor de afhandeling. Daarnaast moet, waar nodig, door het Instituut sturing worden gegeven aan de informatie en gegevens die burgers invullen. Zo voorkomen we dat er te veel informatie bij het Instituut binnenkomt die vervolgens ook weer verwerkt moet worden.

Deze inrichting kan worden getoetst in de DPIA die, indien dit nodig is, door het privacyteam wordt opgesteld

5 Technische en organisatorische maatregelen

De AVG geeft aan dat er technische en organisatorische maatregelen genomen moeten worden om gegevens te beschermen.⁷ Hierdoor worden er privacy eisen gesteld aan systemen. Welke privacybeschermende strategieën gebruikt worden, hangt bijvoorbeeld af van het systeem dat gebruikt gaat worden voor de verwerking. In de literatuur zijn acht verschillende strategieën ontwikkeld die helpen bij het opstellen van concrete ontwerpisen.⁸ Dit noemen we de privacy ontwerp strategieën. Het Instituut streeft er naar om deze strategieën in te zetten om zijn informatiesystemen 'PbD-proof' te maken.

5.1 Privacy by Design Strategieën

De gedachten ('strategieën') achter PbD kunnen worden gebruikt als richtlijnen bij het ontwerpen van systemen en om bestaande systemen of regelingen zo privacy vriendelijk als mogelijk in te stellen. Door PbD als uitgangspunt te nemen zorgen we ervoor dat er keuzes worden gemaakt die de bescherming van persoonsgegevens bevorderen. De acht strategieën voor PbD zijn onderverdeeld in twee verschillende categorieën, namelijk data georiënteerde en organisatorische strategieën.

Data georiënteerde strategieën

Deze strategieën zijn meer technisch van aard. Ze zien op de inachtneming van privacy tijdens de verwerkingsprocessen.

- Het minimaliseren van data.
- Het scheiden van data
- Het abstraheren van data
- Het beschermen of verstoppen van de data

Organisatorische strategieën

Deze strategieën zijn gericht op de processen rond de verwerking van persoonsgegevens. Deze zijn meer organisatorisch van aard.

- Informeer: informeer de betrokkene over welke persoonsgegevens van hem of haar worden verwerkt.
- Geef controle: zorg ervoor dat de betrokkene, mede door de juiste informatie te geven ook controle kan uitoefenen op zijn of haar data.
- Dwing af: Dwing af dat privacy op een juiste manier wordt gewaarborgd door processen zo in te richten dat hieraan voldaan moet worden.
- Demonstreer: Laat zowel intern als extern duidelijk blijken op welke manieren privacy is gewaarborgd.

Deze organisatorische strategieën vragen bewustzijn van alle medewerkers. Door stromen en processen met persoonsgegevens te herkennen en identificeren kunnen we ervoor zorgen dat de informatievoorziening op een juiste manier plaats vindt en dat op relevante punten kan worden gecontroleerd of aan de wetgeving wordt voldaan.

⁷ Zie artikel 25 AVG.

⁸ Hoepman, J.H. (2019). Privacyontwerpstrategieën, *Het Blauwe Boekje*, p.1-4.
<https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf>.

Privacy by design – Toetsingskader

Dit document dient als toetsingskader om te beoordelen in hoeverre een (nieuwe) gegevensverwerking voldoet aan de beginselen van Privacy by Design (en Default). De criteria die gebruikt worden voor dit toetsingskader zijn afgeleid van de zeven principes van Privacy by Design van Ann Cavoukian.¹ Onder elk beginsel zijn een aantal toetsingscriteria uitgewerkt. Iedere vraag dient aan de hand van een kleur beantwoord te worden. Hierbij dient een korte toelichting gegeven te worden.

Kleurensysteem

Rood: helemaal niet aanwezig. Spoedeisend, risico groot

Oranje: deels aanwezig, maar nog niet voldoende

Geel: aanwezig, maar behoeft nog enige aandacht: er zijn nog verbeterpunten of zaken die aangevuld moeten worden

Groen: aanwezig en van goede kwaliteit.

Bevindingen zien op de feitelijke status. Bij de **opmerkingen** staan aanbevelingen opgenomen.

¹ <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>

Handel proactief en denk vooraf na over privacyrisico's en verklein deze risico's door vooraf maatregelen te implementeren.

Voorkom problemen in plaats van ze achteraf op te lossen

	Bevinding	Opmerking
Is er een duidelijke en volledige procesbeschrijving aanwezig, voor zover mogelijk in de fase waarin het project zich bevindt?	xx	xx
Is vastgelegd waarom bepaalde alternatieven die mogelijk privacyvriendelijker zijn niet gekozen zijn?	xx	xx
Is er voorafgaand aan de gegevensverwerking beoordeeld of een DPIA moet worden uitgevoerd?	xx	xx
Indien geoordeeld is dat een DPIA nodig is: staat deze op de planning?	xx	xx.
Zijn medewerkers op de hoogte van de privacyregels omtrent deze nieuwe gegevensverwerking?		

Streef naar een maximaal niveau van privacy door de standaardinstellingen van het product of de dienst op het maximale niveau qua gegevensbescherming in te stellen.

Privacy is automatisch gewaarborgd zonder dat de gebruiker iets hoeft te doen

	Bevinding	Opmerking
Worden alleen de strikt noodzakelijke gegevens verzameld? (Is het proces zo ingericht dat er rekening wordt gehouden met doelbinding en dataminimalisatie?)	xx	xx

Worden de doelen van de gegevensverwerking vooraf duidelijk gecommuniceerd? (Transparantie en informatie)	xx	xx
Zijn de standaardinstellingen privacyvriendelijke ingericht? (bijv. Geen vooraf aangevinkte vinkjes/opt-out/autorisatie rollen toegekend)	xx	xx
	xx	xx.

Veranker PbD in het ontwerp en leg de overwegingen vast zodat deze getoetst kunnen worden.

Privacy is een integraal onderdeel van systemen en processen

	Bevinding	Opmerking
Is er documentatie aanwezig over de overwegingen met betrekking tot PbD?	xx	xx
Is privacy vanaf de start meegenomen in het ontwerp van systemen/processen?	xx	xx
Vraag 3	xx	xx
Vraag 4	xx	xx.

Privacy mag niet ten koste gaan van andere rechten en waarborgen.

Privacy en andere doelen (zoals veiligheid of gebruiksgemak) worden gecombineerd, niet als tegenstellingen behandeld

	Bevinding	Opmerking
Is duidelijk in kaart gebracht welke andere rechten en waarborgen	xx	xx

van betrokkenen belangrijk zijn? (let op dat dit ook gedocumenteerd moet zijn)



Zijn alle belangen (veiligheid, gebruiksgemak, privacy) meegewogen in de afweging?



xx

Zijn er alternatieven bekeken om het evenwicht/de functionaliteit beter te behouden?



xx

Vraag 4



xx.

Pas PbD toe gedurende de gehele levenscyclus van een persoonsgegeven, niet alleen tijdens de ontwerpfase.

Privacybescherming geldt over de hele levenscyclus van gegevens (van verzameling tot verwijdering)

	Bevinding	Opmerking
Is een proces ingericht waarbinnen periodiek gecontroleerd wordt of de vastgestelde maatregelen zijn uitgevoerd en of de lijst met risico's nog steeds relevant en volledig is?	xx	xx
Zijn er passende maatregelen genomen om de gegevens te beveiligen? (bewaartermijnen, encryptie, autorisatie, logging etc.) <i>Deze maatregelen moeten afgestemd zijn op de gevoeligheid van de gegevens</i>	xx	xx.
Worden medewerkers voortdurend geïnformeerd over de regels omtrent de		

privacy van het proces?		
Worden gegevens na afloop van het doel veilig verwijderd of geanonimiseerd?		

Documenteer de processtappen van PbD zodat beoordelingen en besluiten transparant en zichtbaar zijn.

Verwerking is zichtbaar, controleerbaar en inzichtelijk voor betrokkenen en toezichthouders

	Bevinding	Opmerking
Is er een goed ingevulde PbD vragenlijst beschikbaar?	xx	xx
Is er duidelijk welke persoonsgegevens worden verwerkt en beschermd?	xx	xx
Is vastgelegd waarom bepaalde keuzes zijn gemaakt?	xx	xx
Is er een klachtenprocedure ingericht en zijn betrokkenen hierover geïnformeerd?	xx	xx.

Stel altijd het belang van de betrokkene centraal.

De gebruiker staat centraal, met duidelijke keuzes en controle over eigen gegevens

	Bevinding	Opmerking
Is het proces zo ingericht dat betrokkenen hun rechten effectief uit kunnen oefenen?	xx	xx
Is het systeem gebouwd op een manier die het voor medewerkers	xx	xx

makkelijk maakt om informatie uit te vragen of aan te passen?		
Worden betrokkenen in de privacyverklaring voorgelicht over de verwerking van hun gegevens voor het nieuwe project? Leg indien dit niet het geval is uit waarom dit niet gebeurd.	xx	xx
Indien de verwerking gebaseerd is op toestemming van de betrokkene: is het process hieromtrent zo ingericht dat de betrokkene vrije en specifieke toestemming kan geven?	xx	xx.



Privacybeleid



Colofon

Contactpersoon	5.1.2e5.1.2e5.1.2e Privacy@schadedoormijnbouw.nl Instituut Mijnbouwschade Groningen Afdeling Informatievoorziening Cascadeplein 10, 9726 AD Groningen 0800 4444 111
Auteurs	5.1.2e
Versie	2.0
Status	Definitief
Bijlage(n)	3

Versie	Datum	Door	Wijzigingen
D 1.0	1 februari 2022	5.1.2e	Beleid vastgesteld.
D 1.1	29 augustus 2024	5.1.2e	Privacybeleid in concept herzien
D 2.0	10 december 2024	5.1.2e	Herziene privacybeleid vastgesteld.



Inhoudsopgave

Afkortingenlijst 5

Voorwoord 6

1. Inleiding 7

- 1.1 Toelichting 7*
- 1.2 Leeswijzer 7*
- 1.3 Scope en relatie tot ander beleid 8*
- 1.4 Geldigheid en eigenaarschap 9*
- 1.5 Wijzigingen n.a.v. audit ADR en zelfevaluatie 10*

2. Het Instituut en privacy 12

- 2.1 Taak en opdracht 12*
- 2.2 Kernwaarden van het Instituut 12*
- 2.3 Kaders 13*
- 2.4 Positie privacy 13*
- 2.5 Doel en reikwijdte privacybeleid 14*
 - 2.5.1 Doel 14*
 - 2.5.2 Reikwijdte 14*
- 2.6 Relevante wetgeving 14*
 - 2.6.1 Inkleding wettelijke taak 14*
 - 2.6.2 Privacy wet- en regelgeving 14*
 - 2.6.3 Aanverwante wet- en regelgeving 15*

3. Privacyprincipes 16

- 3.1 Visie op privacy 16*
- 3.2 Uitgangspunten 16*

4. Governance 19

- 4.1 Achtergrond: three lines model 19*
- 4.2 Rollen en verantwoordelijkheden 20*
 - 4.2.1 Het bestuur 20*
 - 4.2.2 Het lijnmanagement 20*
 - 4.2.3 Functionaris Gegevensbescherming (FG) 20*
 - 4.2.4 Hoofd Informatievoorziening 20*
 - 4.2.5 Privacy Officer (PO)/Coördinator Informatiebeveiliging en Privacy (Coördinator IB&P) 21*
 - 4.2.6 Chief Information Security Officer (CISO) 21*
 - 4.2.7 (Information) Security Officer (ISO of SO) 21*
 - 4.2.8 De medewerker (interne en externe) 21*
 - 4.2.9 Dienstenleverancier/externe partijen 22*

5. Overlegstructuren 23

- 5.1 Concernbreed 23*



5.2 Intern 23

5.3 Escalatielijnen 23

6. Beheersing van privacy 24

6.1 PDCA-cyclus privacy 24

6.2 Privacy volwassenheid en strategie 24

6.3 Privacy Baseline 25

6.4 Bewustwording en training 25

6.5 Activiteiten gedurende het jaar 26

6.5.1 Beheersing privacy 26

6.5.2 Toezichtactiviteiten Functionaris Gegevensbescherming 27

6.6 Operationele activiteiten 27

6.6.1 Operationeel privacybeleid 27

6.6.2 AVG-register 28

6.6.3 Overeenkomsten 28

6.6.4 Privacyverklaring 28

6.6.5 Documentatie 28

6.6.6 DPIA 29

6.6.7 Privacy in projecten 29

6.6.8 Verwerkers 29

6.6.9 Bewustwordingsprogramma 30

6.6.10 Kwaliteit, interne controles en audits 30

6.6.11 Kennispartners EZK en RVO 30

Bijlage 1 – Verklaring van begrippen 31

Bijlage 2 - Beleid doorgifte 32

Bijlage 3 - Beleid Privacy by design en default 33



Afkortingenlijst

(I)SO	(Information) Security Officers
ADR	Auditdienst Rijk
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemene wet bestuursrecht
BIO	Baseline Informatiebeveiliging Overheid
CISO	Chief Information Security Officer
Coördinator IB&P	Coördinator Informatiebeveiliging & Privacy
Def	Ministerie van Defensie
DPIA	Data protection impact assessment
EZK&LNV	Ministerie van Economische Zaken en Klimaat en Landbouw, Natuur en Voedselkwaliteit
EZK	Ministerie van Economische Zaken en Klimaat en Landbouw
FG	Functionaris Gegevensbescherming
Fin	Ministerie van Financiën
I&W	Ministerie van Infrastructuur en Waterstaat
IB	Informatiebeveiliging
IB&P	Informatiebeveiliging en privacy
IV	Informatievoorziening
MT	Managementteam
PEAG	Parlementaire enquête aardgaswinning Groningen
PO	Privacy Officer
RVO	Rijksdienst voor Ondernemend Nederland
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VWS	Ministerie van Volksgezondheid, Welzijn en Sport



Voorwoord

Voor u ligt het privacybeleid van het Instituut Mijnbouwschade Groningen (Het Instituut). Inherent aan de werkzaamheden is het voor het Instituut noodzakelijk om persoonsgegevens te verwerken van burgers en medewerkers. Van het Instituut mag verwacht worden dat het de privacyrechten van betrokkenen waarborgt. De invoering van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018 onderstreept dit nog eens. Om de waarborging te ondersteunen is in dit document het privacybeleid van het Instituut vastgelegd: de privacy principes waar iedereen ons op kan aanspreken. De belangen van burgers en medewerkers staan daarbij centraal: bij het Instituut zijn uw persoonsgegevens in goede handen.

Het privacybeleid wordt toegepast binnen alle organisatieonderdelen van het Instituut. Dit beleidsdocument is gebaseerd op het privacybeleid van het ministerie van Economische Zaken en Klimaat en het ministerie van Landbouw, Natuur en Voedselkwaliteit (EZK/LNV). Het beleid van EZK/LNV, waaronder het Instituut als zelfstandig bestuursorgaan ressorteert, is als raamwerk gebruikt voor de vormgeving van het privacybeleid van het Instituut. Hiermee zijn beleidsrichtlijnen vastgesteld die nauw aansluiten op de organisatie en tevens voldoen aan het gestelde normenkader.

Het beleid is opgesteld door de privacy verantwoordelijken van het team IB&P van het Instituut en is voorgelegd aan de Functionaris Gegevensbescherming. Voor vragen over het beleid en de betekenis ervan voor specifieke organisatieonderdelen kan contact worden opgenomen met de Privacy Officers van het Instituut of de Coördinator Informatiebeveiliging & Privacy.

Eind 2023 is het Instituut door de Auditdienst Rijk (ADR) onderzocht op het gebied van privacy en gegevensbescherming. De ADR heeft het Instituut getoetst op zijn huishouding omtrent de bescherming van persoonsgegevens. In 2024 heeft de ADR haar bevindingen gedeeld met het Instituut. Naar aanleiding van deze audit en een zelfevaluatie wordt dit beleidsstuk op bepaalde punten herzien. Ook worden aanvullende beleidstukken als bijlage gehecht aan dit beleid.

Groningen, september 2024



1. Inleiding

Gegevens van en over burgers moeten bij het Instituut veilig zijn en hun privacy moet zijn gewaarborgd. Dat betekent dat het Instituut vertrouwelijk omgaat met (persoons)gegevens. Los van het voldoen aan wet- en regelgeving, wil het Instituut een betrouwbare partner zijn, waar persoonsgegevens veilig en verantwoord worden verwerkt bij de uitvoering van zijn publieke taak.

1.1 Toelichting

De Algemene Verordening Gegevensbescherming (AVG) en het privacybeleid vragen om een zorgvuldige omgang met persoonsgegevens binnen de organisatie. Dit komt tot uiting in het introduceren van duidelijke principes en gedragsregels. Deze principes en gedragsregels dragen bij aan de bewustwording van management en medewerkers, maar nog belangrijker: ze zetten de burger en de medewerker centraal bij de bescherming van persoonsgegevens.

Privacy gaat meer over gedrag dan over procedures, meer over risico's beheren en inzichtelijk maken dan over maatregelen en techniek, meer over 'nog eens nadenken' dan over 'we doen dat altijd al zo'. De AVG stelt de betrokkene centraal en de risico's die de betrokkene loopt als gegevens over hem/haar worden opgeslagen. Ook de invloed van de betrokkene op de persoonsgegevens die zijn opgeslagen is groter en de autonomie van de betrokkene is stevig verankerd binnen de organisatie en de AVG.

Wanneer in dit document wordt gesproken over privacy, dan wordt de informationele privacy bedoeld. Informationele privacy gaat over het verwerken en verzamelen van persoonlijke data, bijvoorbeeld financiële gegevens, medische gegevens, contactgegevens, etc.

Het privacybeleid van het Instituut is geïnspireerd door het privacybeleid van EZK/LNV, waarbij is getracht een balans te vinden tussen de kernwaarden van het Instituut waarbij de rijksbrede normen en waarden zo veel mogelijk in stand worden gehouden.

1.2 Leeswijzer

Het privacybeleid van het Instituut bestaat uit een aantal secties voor verschillende lezersgroepen. Het eerste deel van het beleid is bestemd voor alle medewerkers van het Instituut en alle bedrijfsonderdelen en geeft op een hoog abstractieniveau aan waar het Instituut voor wil staan en wat het wil uitdragen.

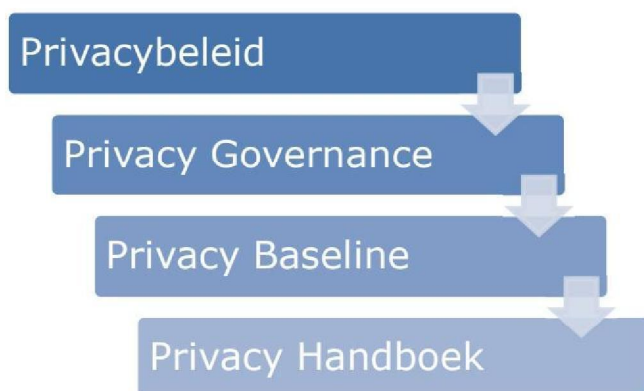
Het tweede deel van het beleid, de Privacy Governance, beschrijft de inrichting van sturing, regie en beheer en is relevant voor de medewerkers die vakmatig betrokken zijn bij de implementatie en het onderhoud van privacyrichtlijnen en -management. Ook de privacystrategie is onderdeel van de Governance.

Het derde deel, de Privacy Baseline, omvat het normenkader en het toetsingskader: een opsomming van de eisen die privacywet- en regelgeving aan de organisatie stelt. Het is wederom gericht op de vakmensen, maar ook op het lijnmanagement dat verantwoordelijk is voor de implementatie en onderhoud van de wet- en regelgeving binnen zijn verantwoordelijkheden. De Privacy Baseline wordt door meerdere ministeries gezamenlijk vastgesteld en is daardoor geen onderdeel van dit document.

Het vierde deel, het Privacy Handboek, is een intern privacybeleid en bevat de praktische vertaalslag van de uitgangspunten uit dit beleid naar de dagelijkse omgang met persoonsgegevens door alle medewerkers binnen de organisatie. Het Privacy Handboek stelt de vraag centraal: hoe kan ik in mijn dagelijkse werkzaamheden bijdragen aan de bescherming van persoonsgegevens? Het Privacy



Handboek vormt de leidraad voor medewerkers in de omgang met persoonsgegevens. Vanwege het veranderlijke karakter is het Privacy Handboek niet opgenomen in dit document.

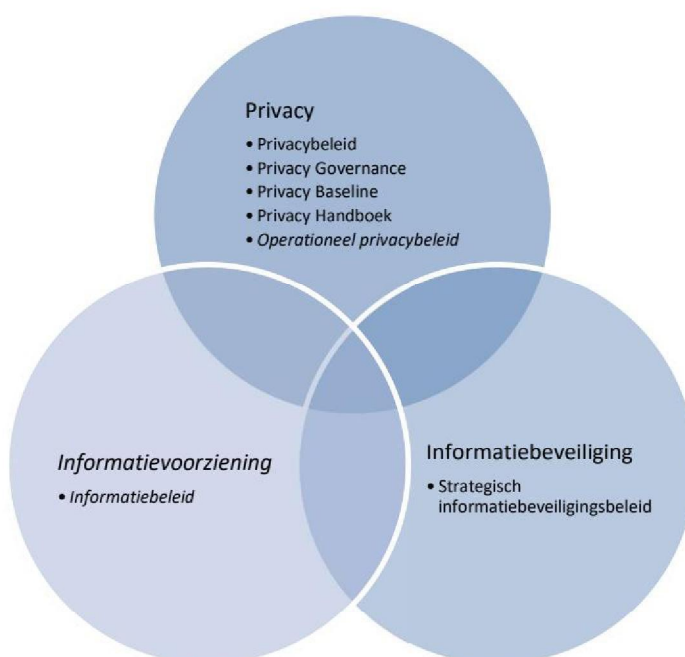


Er dient opgemerkt te worden dat het Instituut ook beschikt over een operationeel privacybeleid, zoals het beleid voor logging en monitoring en het opnemen en bewaren van telefoongesprekken. Een overzicht van al het operationele beleid met betrekking tot privacy wordt bijgehouden door de Privacy Officer en is aldaar op te vragen. Omdat het operationeel privacybeleid voor een beperkte groep medewerkers van toepassing is en sterk samenhangt met de (soms snel wisselende) werkprocessen, wordt het operationeel privacybeleid in dit document verder buiten beschouwing gelaten, ondanks dat deze documenten als aanvullende normenkaders kunnen dienen.

Naast bovenstaand beleid bestaan er andere specifieke documenten waarin is vastgelegd hoe het privacybeleid op strategisch en operationeel niveau uitgevoerd dient te worden. Omdat deze documenten uitvoering geven aan het beleid worden deze documenten niet als beleidsstukken gezien.

1.3 Scope en relatie tot ander beleid

Naast het privacybeleid bestaat het informatiebeleid en het informatiebeveiligingsbeleid van het Instituut. Het informatiebeleid gaat over de informatievoorziening binnen het Instituut. Vanuit privacy en informatiebeveiliging bestaat een gedeeld belang met informatievoorziening, omdat het gedegen vormgeven van de informatiehuishouding vereist is voor een goede uitvoering van privacy en informatiebeveiliging. Elementen zoals privacy by design en default en security by design en default moeten onderdeel zijn van de systemen van het Instituut. Hiermee draagt het Instituut zorg voor veilige verwerkingen van persoonsgegevens.



Privacy en informatiebeveiliging hebben tevens andere overlappende belangen. Privacy heeft als doel (persoons)gegevens tegen onrechtmatige toegang, verlies of aantasting te beschermen. Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Het informatiebeveiligingsbeleid is met name relevant voor de passende technische en organisatorische maatregelen die genomen worden om persoonsgegevens te beschermen.

Ook in de praktische uitvoering van het beleid zal het overlappende belang tot uiting komen door gezamenlijk op te trekken en te spreken over 'Informatiebeveiliging & Privacy' (IB&P), bijvoorbeeld als het gaat om bewustwording. Het informatiebeveiligingsbeleid en privacybeleid worden op elkaar afgestemd: bij het wijzigen van één van beide beleidskaders wordt expliciet getoetst of dit in lijn is met het andere beleidskader.

1.4 Geldigheid en eigenaarschap

Het privacybeleid treedt in werking op het moment van vaststelling. Het privacybeleid wordt vastgesteld door de Chief Information Officer (CIO) van het Instituut.

Het beleidsdocument is geldig tot een nieuwe versie is vastgesteld door de CIO. Namens deze beheert de Privacy Officer het document.

Dit document wordt bij wijzigingen in wet- en regelgeving, de missie, visie of strategie van Instituut, de organisatie van Instituut of bij wijziging van het informatiebeveiligingsbeleid geëvalueerd en waar nodig bijgesteld of herzien. In het geval er tussentijds nieuw of aanvullend beleid nodig is, dan kunnen wijzigingen als addendum bij dit document worden gevoegd. De verantwoordelijkheid voor het actueel houden en evalueren van het beleid is belegd bij de Privacy Officers van het Instituut.



Dit privacybeleid wordt gepubliceerd en kenbaar gemaakt aan de betreffende lezersgroepen via de interne communicatiesystemen. Uitgangspunten van dit privacybeleid zullen tevens worden opgenomen in de privacyverklaring op de website van het Instituut www.schadedoormijnbouw.nl.

1.5 Wijzigingen n.a.v. audit ADR en zelfevaluatie

Eind 2023 is de datahuishouding van het Instituut door de ADR onderzocht op het gebied van privacy en gegevensbescherming. In 2024 heeft de ADR haar bevindingen gedeeld met het Instituut en het Instituut is voornemens om deze bevindingen te implementeren, voor zover dat nog niet is gebeurd. Een aantal van deze bevindingen zien toe op wijzigingen in het beleid, zoals:

- 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.
- Maak privacy-gerelateerde wervingsplan en -behoefte onderdeel van het jaarplan om op lange termijn privacykennis en -expertise te borgen binnen het Instituut.

In deze herziene versie van het privacybeleid zullen bovenstaande punten worden verwerkt. Er is een aanvullend beleidsstuk geschreven over privacy by design en default en dit beleidsstuk zal als bijlage worden toegevoegd aan dit beleid alsmede de overige stukken zoals het beleid doorgifte. Tevens zal er onder [paragraaf 3.2](#) een aanvullend uitgangspunt over het verwerken van bijzondere persoonsgegevens worden opgenomen. In [paragraaf 6.4](#) zal er een wervingsplan worden opgenomen om de lange termijn privacykennis en – expertise te borgen binnen het Instituut.

Naast de bevindingen van de ADR, heeft het team IB&P ook een zelfevaluatie uitgevoerd. Daaruit is voortgekomen dat de visie uit hoofdstuk 2 van dit beleid niet meer in lijn is met de huidige missie van het Instituut. De actuele missie van het Instituut is aangepast in 2024 en heet: 'Bouwen aan Herstel'. Bij die missie hoort ook een nieuwe kernopgave. Met deze herziening wordt er een vertaalslag gemaakt van deze missie van het Instituut naar de privacyvisie van het Instituut.



Sectie 1

Privacybeleid



2. Het Instituut en privacy

Wat is ons doel?

2.1 Taak en opdracht

Het Instituut is opgericht met als doel schade af te handelen die is ontstaan door bodembewegingen als gevolg van de aanleg of exploitatie van mijnbouwwerken ten behoeve van gaswinning uit het Groningerveld of de gasopslag Norg. Het Instituut voert deze taak uit door als zelfstandig bestuursorgaan te besluiten over aanvragen tot schadevergoeding. Het gaat hierbij niet alleen om de vergoeding van fysieke schade aan gebouwen, maar ook waardedalingen en immateriële schade. Daarnaast worden meldingen van mogelijk acuut onveilige situaties (AOS) bij het Instituut gedaan en biedt het Instituut ook herstel in natura aan. In de jaren 2023 en 2024 zijn regelingen zoals Duurzaam Herstel, Immateriële schade voor kinderen en jongeren en Waardedaling Niet Wonen aan het takenpakket van het Instituut toegevoegd.

De eerste opdracht van het Instituut was om onafhankelijk, rechtvaardig, ruimhartig en voortvarend mijnbouwschade af te handelen. Het Instituut deed dat met oog voor de menselijke maat. Het Instituut had dan ook als missie om bij te dragen aan herstel van de schade én van dat gevoel waaraan het de bewoners en ondernemers soms ontbrak. De bewoner moest in alle processen van het Instituut weten en merken: **"Ze hebben voor mij gedaan wat ze konden"**. Dit deed het Instituut door schade af te handelen, maar ook te ondersteunen tijdens het proces en nazorg te geven.

Met bovenstaande doelstelling heeft het Instituut een adequaat antwoord proberen te geven op vraagstukken van schade, onveiligheid, groeiende onzekerheid, stress, leed en verdriet. Die pogingen zijn volgens de parlementaire enquêtecommissie aardgaswinning Groningen uit 2023 (de PEAG) gedeeltelijk succesvol gebleken. De werkwijze van het Instituut was te juridisch en complex en leidde in sommige gevallen tot onverklaarbare verschillen.

Om deze onverklaarbare verschillen op te lossen heeft het Instituut een nieuwe visie bedacht: **'Bouwen aan Herstel'** en de kernopgave uit deze visie luidt als volgt: 'Onze kernopgave is het afhandelen en zoveel mogelijk **daadwerkelijk herstellen** van schade, die mensen en gebouwen oplopen en hebben opgelopen, in het effectgebied. Daarbij staan aanvragers centraal en ligt onze focus op waar de impact van de gevolgen van de gaswinning het grootst is. Wij doen dat **mild, menselijk, makkelijk, professioneel** en **deskundig**. Zo bouwt het Instituut mee aan perspectief voor de regio en zijn bewoners'.

2.2 Kernwaarden van het Instituut

Naast de positionering en opdracht om te Bouwen aan Herstel en het daadwerkelijk herstellen van schade zijn de kernwaarden uit de kernopgave van het Instituut dus:

- **Mild**
- **Menselijk**
- **Makkelijk**
- **Professioneel**
- **Deskundig**

De kernwaarden van het Instituut kennen een eigen invulling op privacygebied.

Medewerkers van het Instituut zijn **mild** bij de uitvoering van de werkzaamheden. Mild houdt in dat het Instituut schade ruimhartig vergoed en bij fysieke schade de causaliteit deels wordt losgelaten. Binnen de context van privacy betekent dit dat het Instituut op een vriendelijke en meegaande manier omgaat met persoonlijke gegevens van burgers en medewerkers. Het Instituut draagt er



zorg voor dat het privacybeleid en -procedures duidelijk en toegankelijk zijn, en dat doet het Instituut door bij het verwerken van persoonsgegevens alleen het strikt noodzakelijke te verwerken, waarbij altijd respect getoond wordt voor de persoonlijke levenssfeer van individuen.

Het Instituut benadert burgers en werkt op een **menselijke** manier. Menselijk duidt op het respecteren van de menselijke waardigheid en het tonen van compassie. Het Instituut erkent en waardeert het belang van privacy voor het individuele welzijn. Daarom realiseert het Instituut dit door de privacyrechten van individuen te respecteren, hen te informeren over hoe hun gegevens worden gebruikt, en hen controle te geven over hun eigen informatie.

De processen en diensten van het Instituut zijn **makkelijk** en toegankelijk. Makkelijk houdt in dat processen niet onnodig complex worden gemaakt. Het Instituut waarborgt privacyprocessen op een manier die eenvoudig en transparant is. Het Instituut biedt op zijn platformen gebruiksvriendelijke privacyinstellingen aan, hanteert duidelijk en eenvoudig te begrijpen privacyverklaringen en procedures, en reageert snel op verzoeken om toegang tot, correctie van of verwijdering van persoonlijke gegevens.

Het Instituut handelt te allen tijde **professioneel**. Professioneel impliceert een hoge mate van betrouwbaarheid, bekwaamheid en verantwoordelijkheid. Daarom neemt het Instituut privacy serieus en laat hij zien dat hij de hoogste normen van gegevensbescherming naleeft. Het Instituut laat zich daarom regelmatig auditen op zijn privacyprocessen, implementeert robuuste beveiligingsmaatregelen en zorgt dat zijn personeel continue wordt opgeleid en bewust wordt gemaakt op het gebied van privacy.

De medewerkers van het Instituut zijn **deskundig**. Dat betekent dat het Instituut de juiste kennis en expertise inzet in zijn operaties. Op het privacyvlak houdt dit in dat er gespecialiseerde privacymedewerkers worden aangesteld, dat er voortdurend wordt geïnvesteerd in de nieuwste technologieën voor gegevensbescherming, en dat er proactief wordt ingespeeld op nieuwe ontwikkelingen en bedreigingen op het gebied van privacy.

Doordat het Instituut deze kernwaarden in de context van privacy omarmt, toont het Instituut niet alleen aan dat het waarde hecht aan gegevensbescherming, maar dit ook op een manier doet die aansluit bij de missie 'Bouwen aan Herstel' en daadwerkelijk herstel.

2.3 Kaders

In de uitvoering van de taken handelt het Instituut langs de lijn van 'Bouwen aan Herstel'. Dat houdt niet alleen in dat de schade daadwerkelijk ook hersteld wordt, maar dat het vertrouwen van de Groningse burger in de overheid eveneens wordt hersteld. Het Instituut blijft daarom zijn taak uitvoeren zolang er door bodembeweging door gaswinning in het Groningenveld en de gasopslag Norg blijft bestaan. Hierbij waarborgt het Instituut de gegevens van de burgers. De basis voor het bestaan van het Instituut en het afhandelen van de schade ligt in de Tijdelijke Wet Groningen. Zie voor meer informatie over wettelijke kaders hoofdstuk 2.6.

2.4 Positie privacy

'**Bouwen aan Herstel**' betekent de belofte om de schade daadwerkelijk te herstellen, maar ook het streven om het vertrouwen van de burger niet verder te schaden. De bescherming van persoonsgegevens maakt een groot onderdeel uit van deze belofte.

Binnen het Instituut is het namelijk belangrijk dat de persoonsgegevens van betrokkenen in goede handen zijn. Dit betekent dat het Instituut de privacybelangen van de betrokkenen zorgvuldig in acht neemt. Naleving van de toepasselijke privacy wet- en regelgeving is hierbij vanzelfsprekend. Dit privacybeleid is een richtinggevend document voor het in acht nemen van de privacybelangen van



alle betrokkenen in alle processen binnen het Instituut waarmee de kernwaarden van het Instituut worden ondersteund.

2.5 Doel en reikwijdte privacybeleid

2.5.1 Doel

Het doel van het privacybeleid is het veiligstellen van de privacy van alle betrokkenen in alle processen door het hanteren van in de gehele organisatie toepasbare privacyuitgangspunten. Het privacybeleid beoogt te bevorderen dat alle betrokkenen erop kunnen vertrouwen dat persoonsgegevens en (vertrouwelijke) informatie integer en in lijn met toepasselijke wet- en regelgeving worden verwerkt.

2.5.2 Reikwijdte

Het privacybeleid is gericht op het Instituut als organisatie en op de gehele bedrijfsvoering van het Instituut. Hieronder vallen alle activiteiten in de schadeafhandelingsprocessen, alle (ondersteunende) bedrijfsactiviteiten en alle betrokkenen en stakeholders die hiermee te maken hebben, zoals medewerkers, aanvragers en externe relaties.

2.6 Relevante wetgeving

Naast de in hoofdstuk 2.3 gegeven kaders waarbinnen het Instituut zijn taken uitvoert, bestaat er specifieke wetgeving op het gebied van privacy waar het Instituut zich te allen tijde aan dient te houden bij het uitvoeren van de toegekende taken.

2.6.1 Inkleding wettelijke taak

De grondslag voor het bestaan van het Instituut en het afhandelen van de schade ligt in de Tijdelijke Wet Groningen. Bij de uitvoering van de werkzaamheden werkt het Instituut binnen de kaders van het civiele aansprakelijkheids- en schadevergoedingsrecht.

Specifieke werkwijzen, mandaten en volmachten zijn vastgesteld in daarvoor gegeven besluiten. Een overzicht van de besluiten die van toepassing zijn op de inkleding van de wettelijke taak van het Instituut is op te vragen via de Privacy Officer.

2.6.2 Privacy wet- en regelgeving

Wet- en regelgeving op het gebied van privacy is terug te vinden in verschillende lagen. Zowel op Europees als op nationaal niveau en in specifieke wetgeving voor bepaalde thema's bestaat privacy wet- en regelgeving, zoals de AVG en de Uitvoeringswet AVG (UAVG). Bij het opstellen van dit privacybeleid is niet alleen naar wetgeving gekeken, maar ook naar uitgangspunten waar het ministerie EZK/LNV voor wil staan en de vertaling ervan naar het Instituut.

De AVG zorgt er voor dat de privacyrechten van betrokkenen worden versterkt en uitgebreid, dat er meer verantwoordelijkheden zijn voor organisaties (denk aan een documentatie- en verantwoordingsplicht) en meer bevoegdheden voor de Autoriteit Persoonsgegevens (de toezichthouder heeft onder andere een boetebevoegdheid).

De AVG gaat niet over de bescherming van *alle* gegevens, maar over de bescherming van *persoonsgegevens*. Persoonsgegevens zijn gegevens die herleidbaar zijn tot natuurlijke personen. Zo kan een dataset geen persoonsgegevens bevatten, maar het combineren van datasets kan ertoe leiden dat deze combinatie van gegevens het mogelijk maken om natuurlijke personen te identificeren. Hierdoor wordt de gecombineerde dataset plots een dataset met persoonsgegevens.



De UAVG bevat aanvullingen op de AVG vanuit de Nederlandse wetgever. In de UAVG staan bijvoorbeeld extra maatregelen opgenomen als het gaat om de invulling van wettelijke plichten en beginselen uit de AVG, zoals aanvullende voorwaarden voor individuele geautomatiseerde besluitvorming.

2.6.3 Aanverwante wet- en regelgeving

Bij het verwerken van de persoonsgegevens voor het uitvoeren van de wettelijke taak is het Instituut gebonden aan de Algemene wet bestuursrecht en de Wet open overheid. Het Instituut is een zelfstandig bestuursorgaan en heeft daardoor tevens verplichtingen vanuit de Kaderwet Zelfstandige bestuursorganen. Gaat het om de omgang met dossiers en de inhoud ervan, dan is het Instituut onder meer gebonden aan de Archiefwet, de Wet algemene bepalingen burgerservicenummer en de Wet basisregistratie personen.



3. Privacyprincipes

Hoe doen we dat?

3.1 Visie op privacy

Het doel van het Instituut is het afhandelen en zoveel mogelijk **daadwerkelijk herstellen** van schade, die mensen en gebouwen oplopen en hebben opgelopen, in het effectgebied. Daarbij staan aanvragers centraal en ligt onze focus op waar de impact van de gevolgen van de gaswinning het grootst is. Wij doen dat **mild, menselijk, makkelijk, professioneel** en **deskundig**.

Vanuit privacyoogpunt worden deze doelen ondersteund door ervoor te zorgen dat betrokkenen erop kunnen vertrouwen dat hun persoonsgegevens en andere vertrouwelijke informatie bij het Instituut in goede handen zijn. Het Instituut bewaakt de organisatiecultuur waarbinnen de privacy van betrokkenen wordt gerespecteerd en ziet toe op het rechtmatige gebruik van informatie. De Privacy Officers delen graag kennis met de organisatie en geeft praktisch advies en begeleiding op het gebied van privacy in de huidige en toekomstige schadeafhandelingsprocessen.

3.2 Uitgangspunten

Het centrale uitgangspunt voor alle gegevensverwerkingen bij het Instituut is:

'Bij het Instituut zijn uw gegevens in goede handen'

Dit garandeert het Instituut door zich te focussen op de volgende acht uitgangspunten:

1. Het Instituut verwerkt alleen persoonsgegevens, als...

Hiervoor een rechtmatige grondslag aanwezig is. Denk hierbij bijvoorbeeld aan de uitvoering van een wettelijke verplichting of wanneer de verwerking noodzakelijk is voor het algemeen belang. Er worden niet meer gegevens opgeslagen dan noodzakelijk is voor het uitvoeren van de taak. Het Instituut kan persoonsgegevens verwerken in het kader van een andere regeling dan waarvoor een aanvraag is gedaan.

2. Het Instituut verwerkt alleen bijzondere persoonsgegevens, als

Hiervoor een rechtmatige grondslag bestaat. Het Instituut mag bijzondere persoonsgegevens verwerken, indien dit noodzakelijk is voor de afhandeling van schade van de bewoners van het aardbevingsgebied. Indien het Instituut bijzondere persoonsgegevens verwerkt, mag het Instituut dit alleen doen wanneer de noodzakelijk technische en organisatorische maatregelen zijn genomen om de verwerking zo veilig mogelijk te laten verlopen.

3. Bij het Instituut staat de betrokkene centraal

De verwerking van persoonsgegevens moet ten dienste van de betrokkene(n) staan. Bij het opzetten en beheren van verwerkingen en registraties kijkt het Instituut altijd naar het belang van de betrokkene en het risico dat hij of zij loopt. De persoonsgegevens worden dan ook niet langer opgeslagen dan strikt noodzakelijk.

4. Het Instituut is transparant, kijk maar...

Het Instituut heeft én geeft inzicht in zijn gegevensverwerkingen. Op de website van het Instituut wordt via de privacyverklaring gecommuniceerd welke gegevensverwerkingen er zijn en welke



persoonsgegevens daarvoor worden gebruikt. Het taalgebruik van het Instituut in de communicatie naar betrokkenen is daarbij begrijpelijk en toegankelijk.

5. Het Instituut waarborgt de rechten in het kader van privacy

Het Instituut houdt persoonsgegevens juist en actueel. Voor alle verwerkingen bij het Instituut kunnen gegevens worden ingezien en gewijzigd, tenzij een wettelijke regeling dit in de weg staat. Het wijzigen of wissen van persoonsgegevens is in principe net zo eenvoudig als het doorgeven van de gegevens. We bewaren persoonsgegevens niet langer dan noodzakelijk is voor de uitvoering van onze wettelijke taak en houden ons aan de vastgestelde bewaartermijnen. Het Instituut houdt oog voor de menselijke maat.

6. Het Instituut is terughoudend in het verstrekken van gegevens aan derden

Het verstrekken van gegevens is aan de orde van de dag. Voor persoonsgegevens gelden in dat kader specifieke en strikte regels. Het Instituut neemt de grootste zorgvuldigheid en terughoudendheid in acht als het gaat om het verstrekken van persoonsgegevens aan derden. Het Instituut verstrekt uitsluitend persoonsgegevens aan derden wanneer dit noodzakelijk is voor het uitvoeren van de schadeafhandelingsprocessen. Gegevensverstrekking geschiedt uitsluitend wanneer daarvoor een wettelijke grondslag bestaat.

7. Bij het Instituut zijn gegevens veilig

Het Instituut neemt passende technische en organisatorische maatregelen bij de opslag en verwerking van gegevens. Voorafgaand aan het verzamelen, verstrekken of anderszins verwerken maakt het Instituut een analyse en neemt maatregelen zodat persoonsgegevens altijd beveiligd zijn. Risicovolle verwerkingen vinden alleen plaats nadat een risicoanalyse is uitgevoerd.

8. Het Instituut toont zijn principes aan

Het Instituut maakt voor iedereen zichtbaar dat ze zich houdt aan bovenstaande principes. Toezichthouders, politiek en publiek mogen het Instituut altijd vragen om uitleg en uitwerking van deze principes.



Sectie 2

Privacy Governance



4. Governance

Wie doet wat?

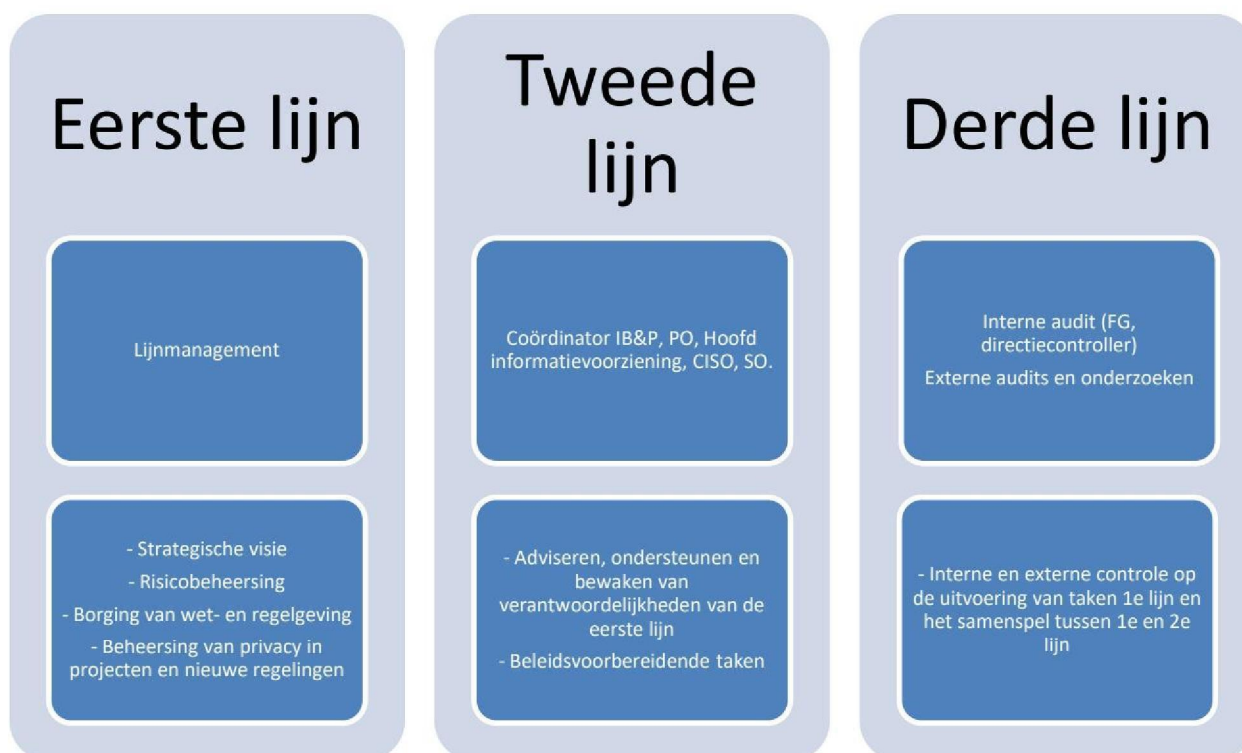
Binnen het Instituut zijn er meerdere functionarissen die zich bezighouden met privacy. Voor het Instituut zijn de rollen en verantwoordelijkheden als volgt belegd.

4.1 Achtergrond: three lines model

Binnen het Instituut wordt gebruik gemaakt van het concept 'three lines model'. In dit model is het lijnmanagement als eerste lijn verantwoordelijk voor de strategische visie, de risicobeheersing en ook voor het borgen van de aantoonbare naleving van wet- en regelgeving op het terrein van privacybescherming. De beheersing van privacy in projecten en nieuwe regelingen vallen hier ook onder.

Binnen de tweede lijn opereren de Coördinator Informatiebeveiliging & Privacy (Coördinator IB&P), Privacy Officers (PO), Chief Information Security Officer (CISO) en Security Officers (SO), die de eerste lijn adviseren en de naleving van de verantwoordelijkheden van de eerste lijn bewaken. Ook bepaalde beleidsvoorbereidende taken en het organiseren van interne risicoanalyses zijn taken van de tweede lijn.

De derde lijn wordt ingevuld door interne audit rollen zoals deze worden uitgeoefend door de Functionaris Gegevensbescherming (FG), de directiecontroller en de interne auditors. Ook externe audits en onderzoeken zijn onderdeel van de derde lijn.



Een aantal partijen hebben een toezichthoudende rol die relevant is met betrekking tot privacy:



- Het Ministerie EZK/LNV houdt in de rol van eigenaar toezicht op het Instituut als zelfstandig bestuursorgaan. Deze rol is beschreven in de Kaderwet Zelfstandig Bestuursorganen en de Tijdelijke wet Groningen.
- De Autoriteit Persoonsgegevens is de toezichthouder op het gebied van privacy.

4.2 Rollen en verantwoordelijkheden

4.2.1 Het bestuur

Privacy is een lijnverantwoordelijkheid. Dat betekent dat de verantwoordelijkheid van privacy begint bij de voorzitter van het bestuur. Bestuursleden hebben een specifieke portefeuille en de portefeuillehouder Informatiebeveiliging & Privacy (IB&P) is het eerste aanspreekpunt.

- Het bestuur ondersteunt actief privacy bij het Instituut door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor privacy toe te kennen en te erkennen.
- Het bestuur stelt het privacybeleid vast en onderschrijft het belang van een goede omgang met persoonsgegevens door de organisatie.
- Het bestuur kent expliciet (gemandateerde) verantwoordelijkheden voor privacy toe.
- Het bestuur stelt middelen (capaciteit en budget) ter beschikking.

4.2.2 Het lijnmanagement

Privacybescherming is een lijnverantwoordelijkheid.

- Het lijnmanagement waarborgt de vaststelling van privacydoelstellingen.
- Het lijnmanagement waarborgt de naleving van privacy wet- en regelgeving in lijn met gemandateerde verantwoordelijkheden.
- Het lijnmanagement bespreekt minimaal één keer per jaar opzet, bestaan en werking van de privacymaatregelen in het overleg op directieniveau en doet hiervan verslag.
- Het lijnmanagement heeft een intern kwaliteitsmechanisme ingericht om de continue verbetering op privacy te waarborgen. Denk aan de periodieke controle op de juistheid van de verwerkingen die in het Register van verwerkingen opgenomen zijn.
- Het lijnmanagement is bekend met de verwerkingen die onder zijn verantwoordelijkheid vallen en formaliseert de verwerkingen. Zij moeten de verwerkingen ondertekenen.
- Het lijnmanagement stelt criteria op voor de acceptatie van risico's bij niet naleving van de AVG.
- Privacybescherming is aantoonbaar onderdeel van de algehele kwaliteitszorg voor de (bedrijfs-)processen en ondersteunende applicaties.

4.2.3 Functionaris Gegevensbescherming (FG)

- De organisatie heeft een FG aangesteld en diens onafhankelijke rol belegd binnen de organisatie.
- De FG is intern toezichthouder op het gebied van privacybescherming en voert de taken uit die zijn beschreven in artikel 39 AVG.
- De FG heeft voldoende middelen en capaciteit om zijn toezichthoudende en adviserende taken in het kader van de AVG naar behoren uit te kunnen voeren. Hij krijgt geen instructies van anderen met betrekking tot zijn taken.
- De FG moet de verwerkingsverantwoordelijke en de betrokken werknemers informeren en adviseren over hun verplichtingen onder de AVG en andere EU of nationaalrechtelijke privacyregelingen. Hij ziet toe op de naleving van de AVG en adviseert desgevraagd over de PIA. Hij werkt samen met en is contactpersoon voor de Autoriteit Persoonsgegevens.

4.2.4 Hoofd Informatievoorziening

Het Hoofd Informatievoorziening is verantwoordelijk voor de informatievoorziening binnen het Instituut, waaronder de kwaliteitsaspecten van informatie(voorziening) zoals informatiebeveiliging



en privacy. Het Hoofd Informatievoorziening of Chief Information Officer (CIO) ontleent zijn rol aan het CIO besluit van de Rijksdienst. Hij of zij is verantwoordelijk voor:

- het opstellen, beheren en evalueren van het (meerjaren) informatieplan van het Instituut;
- het privacybeleid van het Instituut;
- het gevraagd en ongevraagd adviseren van het lijnmanagement over informatievoorziening en digitalisering;
- het initiëren en uitvoeren van organisatiebrede projecten en verbeterplannen op het gebied van informatievoorziening, informatiebeveiliging en privacy.

Het Hoofd Informatievoorziening kan ook de rol van lijnmanager vervullen, bijvoorbeeld voor de informatiemanagementprocessen van het Instituut.

4.2.5 Privacy Officer (PO)/Coördinator Informatiebeveiliging en Privacy (Coördinator IB&P)

De rol van Privacy Officer is belegd binnen de organisatie. Departementen kunnen een andere benaming geven aan een Privacy Officer, bijvoorbeeld Coördinator IB&P. De Privacy Officers hebben onder andere de volgende taken in portefeuille:

- het opstellen, beheren en evalueren van het privacybeleid;
- het opstellen, beheren en evalueren van het privacyjaarplan;
- ondersteunen (adviseren) van lijnmanagement bij de naleving van de privacywetgeving binnen de organisatie of het eigen organisatieonderdeel;
- uitvoeren en coördineren van de privacywerkzaamheden binnen de gehele organisatie;
- aanspreekpunt zijn voor het netwerk privacy, zowel binnen het eigen organisatieonderdeel als extern, en deelnemen aan het netwerk;
- gevraagd en ongevraagd adviseren over privacygerelateerde onderwerpen;
- inventariseren, beoordelen, bijhouden en melden van organisatiegerelateerde verwerkingen;
- behandelen van privacygerelateerde vraagstukken;
- ondersteunen bij het uitvoeren van DPIA's/privacy risicoanalyses voor de verwerkingen waar het afdelingsmanagement voor verantwoordelijk is;
- rapporteren over de status van privacy binnen de eigen afdeling aan het eigen lijnmanagement;
- contact onderhouden en samenwerken met (teams binnen) afdelingen als Juridische Zaken, Communicatie en Bedrijfsvoering.

4.2.6 Chief Information Security Officer (CISO)

De CISO van het Instituut is onder andere verantwoordelijk voor:

- het opstellen, beheren en evalueren van het informatiebeveiligingsbeleid;
- het ontwikkelen en coördineren van informatiebeveiligingsactiviteiten en -projecten binnen het Instituut waaronder het jaarplan informatiebeveiliging;
- het uitvoeren van en adviseren over risicoanalyses en risico-inschattingen;
- het afhandelen van incidenten met grote impact op de doelstellingen van het Instituut.

4.2.7 (Information) Security Officer (ISO of SO)

De ISO of SO is onder andere verantwoordelijk voor:

- het uitvoeren van en adviseren over risicoanalyses op het gebied van informatiebeveiliging;
- het afhandelen van incidenten en datalekken;
- het bevorderen van veilig gedrag en bewustzijn volgens het bewustwordingsprogramma.

4.2.8 De medewerker (interne en externe)

- De medewerker is zich bewust van de gevoeligheid van de gegevens en de daaraan verbonden risico's en handelt daarnaar.
- De medewerker gebruikt bevoegdheden, informatie en gebruikt onder meer voorgeschreven instrumenten en vastgestelde formats zoals de DPIA en de verwerkersovereenkomst.
- De medewerker is als gebruiker verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de eigen functie.



- De medewerker meldt potentiële datalekken op de wijze als voorgeschreven voor zijn departement geldende privacy en gedragsvoorschriften (denk aan het vastgestelde integriteitsbeleid en de Procedure Datalekken voor het melden van datalekken).
- De medewerker volgt trainingen om zijn bewustzijn en kennis te onderhouden en desgewenst te verdiepen.

4.2.9 Dienstenleverancier/externe partijen

Het Instituut maakt gebruik van verschillende leveranciers en derde partijen. Deze partijen zijn verantwoordelijk voor:

- Het adequaat beveiligen van de door het Instituut afgenomen diensten en/of door het Instituut verstrekte (persoons)gegevens.
- Het informeren van het Instituut over (mogelijke) beveiligingsincidenten en datalekken.
- Jaarlijks rapporteren over de beveiliging van de afgenomen diensten of door het Instituut verstrekte (persoons)gegevens en op verzoek rapporteren over de stand van zaken met betrekking tot de invulling van privacywetgeving door de betreffende partij.
- Het meewerken aan verzoeken om informatie en het uitvoeren van audits, DPIA's en andere onderzoeken afkomstig van het Instituut.

Hierbij dient opgemerkt te worden dat in de relatie verwerkingsverantwoordelijke-verwerker de verwerkingsverantwoordelijke eindverantwoordelijk voor de gegevensverwerking van de verwerking. Op het toezien op het voldoen van deze eisen wordt in hoofdstuk 4.6 verder ingegaan.

Schematisch gezien zien de interne rollen ten opzichte van elkaar er als volgt uit:

