

2.5 Verzenden van gegevens

Het is eenvoudig bestanden te verzenden via je werkmail. Het is echter mogelijk dat deze bestanden persoonsgegevens bevatten van betrokkenen. Wanneer je bestanden via je werkmail verzendt, is het van belang met het volgende rekening te houden:

Intern: Voor het intern verzenden van bestanden via je werkmail naar andere medewerkers, is dit geen probleem indien de bestanden worden verzonden via ons interne netwerk naar de werkmail van een andere medewerker. Let daarbij wel op dat je enkel gegevens verstuurt naar een andere medewerker, die voor deze medewerker noodzakelijk zijn om te ontvangen. Zo mag bijvoorbeeld een medewerker van het Instituut, die hiertoe niet bevoegd is, geen medische gegevens ontvangen van aanvragers vanuit IMS. Verwijs ook altijd naar de systemen waarin de gegevens beschikbaar zijn, indien de medewerker daar ook toegang toe heeft. Dat voorkomt het onnodig verzenden van gegevens. Let er ook op dat collega's niet onnodig in de CC worden meegenomen. Denk er ook aan dat de persoonsgegevens in de mail op een gegeven moment weer verwijderd worden. Twijfel je of je bepaalde gegevens mag afgeven aan een collega? Neem dan contact op met een van onze Privacy Officers.

Extern: Voor het verzenden van bestanden naar externe personen/organisaties is het van belang dat, indien de inhoud van deze bestanden gevoelig is, deze bestanden versleuteld verzonden worden. Denk hierbij aan bestanden waar gegevens van aanvragers en/of medewerkers in staan. Dit kunnen bijvoorbeeld facturen, mailinglijsten, lijsten aan gemeentes of de NCG, Cv's en loonstroken zijn. Versleutel bestanden enkel op een door het Instituut aangeboden wijze. Het veilig versturen van bestanden gebeurt via Pleio. Verstuur bovendien enkel gegevens wanneer hiervoor de juiste afspraken zijn gemaakt met de ontvanger, zoals een verwerkersovereenkomst als dat noodzakelijk is. Of er een verwerkersovereenkomst is gesloten, kun je navragen bij inkoop of de Privacy Officers. Twijfel je of je bestanden mag versturen en/of moet versleutelen, of heb je hier vragen over? Neem dan contact op met een van onze Privacy Officers.

Let op! Verstuur enkel bestanden via je werkmail en het interne netwerk van Instituut, of via Pleio. Verstuur geen bestanden met je privé mail en gebruik geen 'openbare' applicaties zoals Dropbox en GoogleDocs. Download en upload enkel bestanden met je werkapparatuur, en niet met je privé laptop/telefoon/tablet.

2.6 Bewaren van gegevens

Wat betreft het bewaren van gegevens hanteren wij de volgende minimale eisen:

- de gegevens moeten tijdens de opslag voldoende beschermd zijn. Dit is mede afhankelijk van de aard van de gegevens. De bescherming dient te voldoen aan de verplichte wet- en regelgeving. Denk hierbij aan het beveiligd opslaan van documenten op je computer/laptop/smartphone, of het afsluiten van kasten waarin papieren documenten worden bewaard. Wanneer je vragen hebt over het opslaan van gegevens kun je je wenden tot het team Informatiebeveiliging (5.1.2i@schadedoormijnbouw.nl);
- de gegevens moeten opgeslagen worden binnen de EER. Indien gegevens buiten de Europese grenzen worden opgeslagen dan moeten hiervoor speciale afspraken worden gemaakt. Maak daarom nooit zonder overleg gebruik van applicaties van partijen zoals Google en Dropbox;
- het moet bekend zijn waar welke gegevens zijn opgeslagen, dit houdt in dat het duidelijk moet zijn in welke systemen of op welke apparatuur gegevens opgeslagen staan en in welk land; en
- er moet een mogelijkheid zijn om de opgeslagen gegevens over te dragen aan de betreffende persoon over wie de gegevens gaan (recht van dataportabiliteit).

Voor alle gegevens geldt in beginsel dat deze slechts bewaard mogen blijven zolang de gegevens daadwerkelijk voor ons noodzakelijk zijn. In de AVG staan geen concrete bewaartermijn opgenomen, maar het IMG dient zich aan verschillende wettelijke bewaartermijnen te houden zoals de Algemene wet inzake rijksbelastingen. Als je hier meer vragen over hebt, kan je contact met de Privacy Officers opnemen.

3. Datalekken

Ondanks de beveiligingsmaatregelen die binnen het Instituut worden gehanteerd, kan ongeautoriseerde toegang tot gegevens of verlies en/of diefstal van gegevens (een datalek) nooit volledig worden uitgesloten. Een datalek is:

"Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens."

Een datalek kan zich op verschillende wijzen voordoen. Denk bijvoorbeeld aan een laptop die gestolen wordt, papieren dossiers die bij de verkeerde persoon terecht komen, het verzenden van een e-mail met daarin persoonsgegevens naar de verkeerde ontvanger of iemand die onrechtmatig toegang verkrijgt tot onze systemen. Kortgezegd is een datalek alles wat 'verkeerd gaat' met persoonsgegevens. Een datalek ligt altijd op de loer als persoonsgegevens worden verwerkt. Het is immers menselijk om fouten te maken. Het belangrijkste is dan ook dat we met elkaar een datalek op de juiste manier afhandelen.

Om de betrouwbaarheid van het Instituut hoog te houden, vragen wij alle medewerkers alert te zijn op mogelijke verdachte zaken. Met onze beveiligingsmaatregelen en de medewerking van het personeel wordt de kans op een datalek verkleind. Meld het daarom direct indien apparatuur is kwijtgeraakt of gestolen (doe dit ook wanneer het privé apparatuur betreft, maar je hierop wel je werk e-mail hebt geïnstalleerd). Laat het ons uiteraard ook weten wanneer er zich andere situaties voordoen waarbij persoonsgegevens mogelijk gelekt zijn, zoals een verloren USB-stick, klachten van klanten of vreemde meldingen in systemen.

Mocht een dergelijke situatie zich voordoen, laat dit dan direct weten via privacy@schadedoormijnbouw.nl. Wij zullen controleren of het een lek is dat wij moeten melden aan de toezichthouder en/of de betrokken personen. Meer weten over de omgang met datalekken? Zie hiervoor het Protocol Datalekken, welke is op te vragen bij de Privacy Officers en te vinden is op de pagina op PLEK.²

Dossiers

Het kan gebeuren dat er persoonsgegevens of stukken van een andere aanvrager in het verkeerde dossier terechtkomen. In dat geval is er mogelijk sprake van een datalek. Meld dit zo snel mogelijk via privacy@schadedoormijnbouw.nl zodat het privacyteam de juiste acties kan ondernemen, zoals het incident registreren in interne systemen. Neem in deze mail Functioneel Beheer meer, zodat zij zo snel mogelijk het mogelijke datalek kunnen dichten. Het privacyteam zal vertrouwelijk omgaan met je melding en je hier nooit persoonlijk op aanspreken. Heb je het gevoel dat er niet goed wordt omgegaan met je melding, laat het dan weten aan de Functionaris Gegevensbescherming (FG). De FG heeft een onafhankelijke, toezichthoudende functie binnen het Instituut. Samen met de FG kan gezocht worden naar een passende oplossing.

² IMG (plek.co).

Rechten van betrokkenen

Voor iedereen van wie wij persoonsgegevens verwerken is in de privacyverklaring³ op onze website beschreven wat ze van ons kunnen verwachten met betrekking tot het verwerken van persoonsgegevens.

Betrokkenen hebben volgens de wet verschillende rechten. Dit zijn:

- recht op inzage en een kopie van de persoonsgegevens die het Instituut verwerkt;
- recht op rectificatie (bijvoorbeeld wanneer het e-mailadres niet correct is);
- recht op verwijdering (een aanvrager wil bepaalde foto's uit zijn dossier verwijderen);
- recht op beperking van de verwerking (een aanvrager wil dat zijn persoonsgegevens niet meer verwerkt worden totdat op een bezwaar is beslist);
- recht op overdraagbaarheid van gegevens (gegevens worden overgedragen met een andere organisatie);
- recht op bezwaar (geldt bijvoorbeeld voor direct marketing);
- recht om niet aan geautomatiseerde besluitvorming onderworpen te worden.

Het is van belang dat alle medewerkers van het Instituut herkennen wanneer een betrokkene gebruikt maakt van een van zijn of haar rechten. Het Instituut moet namelijk in principe binnen één maand gehoor geven aan een verzoek of dit gemotiveerd af te wijzen. Een voorbeeld is bijvoorbeeld dat een aanvrager is verhuisd en vraagt aan een medewerker van het Serviceloket om zijn adres aan te passen. De desbetreffende medewerker dient dit verzoek zo snel mogelijk door te zetten naar het privacyteam via het algemene e-mailadres privacy@schadedoormijnbouw.nl.

Naast verzoeken van aanvragers is het natuurlijk ook goed mogelijk dat medewerkers een AVG-verzoek doen. Medewerkers zijn immers ook betrokkenen. Indien je bijvoorbeeld bezwaar wil maken tegen een bepaalde verwerking of je een inzageverzoek wil doen, kan je het best hiervoor het algemene e-mailadres van het privacyteam, privacy@schadedoormijnbouw.nl contact opnemen.

Er is een procedure rechten van betrokkenen opgesteld door het privacyteam. In deze procedure worden de rechten in meer detail behandeld. Deze procedure is op te vragen bij de Privacy Officers.

³ <https://www.schadedoormijnbouw.nl/over-het-img/privacyverklaring>.

Overige documenten

3.1 Werkinstructie blurren

Er komen binnen de organisatie van het Instituut steeds vaker verzoeken binnen, waarbij een derde graag stukken wilt ontvangen waarin persoonsgegevens van een ander staan. Dit leidt tot vragen wanneer er bepaalde stukken mogen worden gedeeld en hoe er moet worden omgegaan met de persoonsgegevens die in deze stukken staan.

Vaak heeft een verzoeker een gerechtvaardigd belang om een bepaald stuk in te zien (denk aan de schadehistorie bij de constatering van eerder behandelde schades). Ook zijn er gevallen bekend waarbij een betrokkene te veel (bijzondere) persoonsgegevens aanlevert in een bepaald document. Voor dit soort situaties kan het blurren van persoonsgegevens de uitgelezen optie zijn. Blurren is het onleesbaar, wazig of onzichtbaar maken van (bepaalde) persoonsgegevens in een (digitaal) bestand met behulp van een computer(-programma) of handmatig, bijvoorbeeld met een zwarte stift. Indien er wordt geblurd, dient het geblurde object volledig onherkenbaar te zijn.

De Privacy Officers hebben voor het blurren een werkinstructie opgesteld. In deze werkinstructie staat beschreven wanneer en op welke wijze blurren moet worden toegepast. De werkinstructie is te vinden op de T-schijf of op te vragen bij de Privacy Officers.

3.2 Privacy by Design/privacy by default

Het Instituut dient de beginselen van gegevensbescherming door ontwerp (Privacy by Design) en de standaardinstellingen (Privacy by Default) toe te passen. 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. Het belangrijkste uitgangspunt is dat bij het toepassen van PbD in het hele proces centraal staat dat enkel de gegevens die noodzakelijk zijn verwerkt worden. In het hele proces moeten alle ontwerpkeuzes ook gericht zijn op het enkel verzamelen van die gegevens die noodzakelijk zijn. Denk bijvoorbeeld aan de gegevens die worden gevraagd in invulformulieren: vermijd het uitvragen van optionele informatie en open invulvelden. De Privacy Officers hebben een beleidsstuk opgesteld waarin wordt omschreven hoe het Instituut deze beginselen dient toe te passen. Dit beleidsstuk is te vinden in op de T-schijf of op te vragen bij de Privacy Officers.

3.3 AI-beleid

Binnen het Instituut wordt voor verschillende projecten gebruik gemaakt van artificiële intelligentie (hierna: AI). De AI-verordening is ingetreden op 1 augustus 2024, waarna de meeste verplichtingen uit de AI-Verordening in een overgangperiode van twee jaren trapsgewijs van kracht worden. Dit beleid heeft als doel om het Instituut te helpen bij het maken van de keuze om gebruik te maken van AI bij diverse vraagstukken. Dit stuk moet inzichtelijk maken in welke gevallen het gebruik hiervan gerechtvaardigd verantwoord en conform bijpassende wet- en regelgeving is.

3.4 Awareness

Het team Informatiebeveiliging & Privacy besteedt veel aandacht aan awareness binnen het Instituut. Zo heeft het team een aparte pagina op PLEK, waarin het team tweewekelijks aandacht besteedt aan een bepaald onderwerp wat raakvlak heeft met het team. Daarnaast publiceert het team elk kwartaal een nieuwsbrief. Hierin wordt dieper ingegaan op verschillende onderwerpen die het afgelopen kwartaal hebben gespeeld.

3.5 DPIA's

Het uitvoeren van een Data Privacy Impact Assessment (DPIA) is onder bepaalde voorwaarden verplicht. Een DPIA is een instrument om de privacyimpact van een project of een proces waar persoonsgegevens worden verwerkt, te beoordelen. Door middel van een DPIA kunnen de effecten van de verwerking voor betrokkenen in kaart worden gebracht. Aan de hand van die resultaten kan worden beoordeeld of de effecten voor de betrokkenen aanvaardbaar zijn en/of er maatregelen moeten worden genomen om de effecten te voorkomen of te verkleinen. Bij een DPIA moet vooral worden gekeken naar de (geplande) maatregelen, waarborgen en mechanismen om risico's te beperken en persoonsgegevens te beschermen.

Zodra het privacyteam besluit om een DPIA uit te voeren, wordt contact opgenomen met het projectteam. Hierbij wordt in de meeste gevallen een vragenlijst opgestuurd die ingevuld dient te worden door het projectteam. Aan de hand van de ingevulde vragenlijst en overige informatie wordt door de Privacy Officers onderdeel A van de DPIA gevuld. Dit onderdeel wordt daarna ter review naar het projectteam gestuurd. De Privacy Officers vullen hierna de gehele DPIA in. De DPIA voorzien van een FG-advies wordt tot slot aangeboden ter ondertekening aan de proceseigenaar.

4. FAQ

Wanneer en hoe mogen documenten met betrekking tot de zaak worden gedeeld met betrokken partijen?

Het komt soms voor dat een nieuwe eigenaar bepaalde stukken wilt ontvangen over de woning. Daarnaast is het mogelijk dat een advocaat bepaalde stukken opgevraagd voor een bepaalde procedure voor zijn cliënt. Het IMG kan dan documenten delen zolang dit maar op de zaak betrekking hebbende stukken zijn. Je kan bij Juridische Zaken vragen of bepaalde documenten op de zaak betrekking hebbende stukken zijn. Vanuit privacyperspectief dienen alle niet-noodzakelijke persoonsgegevens in het document te worden gelakt. Dit kan via Adobe.

Waar let ik op als ik wegloop bij mijn bureau?

Wanneer je wegloopt bij je bureau dien je, in het kader van de AVG, rekening te houden met een aantal zaken. Ten eerste is het vergrendelen van je computer/laptop van groot belang. Door het vergrendelen van je elektronische apparaten zorg je ervoor dat willekeurige personen niet bij deze gegevens kunnen komen via jouw apparaat. Hiermee voorkom je datalekken. Zorg er daarnaast voor dat aantekeningen met (persoons)gegevens opgeruimd worden, zodat ze niet zichtbaar zijn voor voorbijgangers. Het is belangrijk dat deze informatie niet per ongeluk ingezien kan worden. Ruim dergelijke gegevens altijd netjes op of bewaar ze uit het zicht.

Digitale bestanden met persoonsgegevens bewaar je goed op de goed beveiligde servers van het IMG. Maak geen gebruik van onbeveiligde servers/Wi-Fi-netwerken of persoonlijke apparaten om aan je werkzaamheden uit te voeren.

Hoe herken ik phishing-mails?

Je bent ze vast wel eens tegengekomen: e-mails die afkomstig zijn van (de CEO van) een bedrijf waarin wordt gevraagd naar persoonlijke gegevens. In werkelijkheid is de e-mail verstuurd door een cybercrimineel die de gegeven informatie wil misbruiken. Phishing is een vorm van internetfraude waarbij cybercriminelen proberen persoonlijke gegevens of wachtwoorden te stelen.

Het is van belang om een phishingmail als zodanig te herkennen. Hierbij zijn een aantal punten waar je op kunt letten.

1. Ten eerste kun je kijken naar het e-mailadres. Is het e-mailadres vaag, onduidelijk of zitten er veel getallen in? Wees dan terughoudend. Het is bijvoorbeeld ook goed mogelijk dat een letter in een cijfer wordt veranderd. Bijvoorbeeld: pietjepuk@schadedoormijnbouw.nl wordt p1etjepuk@schadedoormijnbouw.nl. Stuur in alle deze gevallen de e-mail door naar 5.1.2e@schadedoormijnbouw.nl. De Security Officer zal dan met jou kijken of je op deze mail kan reageren.
2. Ten tweede is de aanhef van belang. Als je wordt aangesproken met algemene termen zoals 'geachte meneer, mevrouw of beste klant', wees dan alert. Als het gaat om een bedrijf of organisatie waar je een bepaalde relatie mee hebt, zal je vaak worden aangesproken met heer of mevrouw (niet beide) gevolgd door je achternaam.
3. Ten derde staat in phishingmails vaak het verzoek om op een link te klikken om persoonlijke gegevens te controleren, bij te werken of aan te vullen. Je kunt ook gevraagd worden om in te loggen in een systeem. Op de valse website of het portaal waar je naar wordt doorverwezen, wordt op deze manier je gegevens verkregen. Klik daarom nooit op links die je niet vertrouwt. Open daarnaast ook

nooit zomaar een bijlage bij een mail die afkomstig is van een e-mailadres dat je niet vertrouwt. Een bijlage in een phishingmail kan ervoor zorgen dat er schadelijke software op jouw computer wordt geïnstalleerd.

Moet ik bijhouden met wie ik persoonsgegevens deel?

Het IMG is verplicht om een verwerkingsregister bij te houden. Dit register is te vinden op <https://www.avgregisterrijksoverheid.nl/>. Het doel hiervan is dat het IMG zijn verwerkingen kan inzien, en om transparant naar de burger toe te zijn. Het verwerkingsregister kan namelijk ingezien worden door de burger, om te kunnen kijken hoe en waar persoonsgegevens worden verwerkt. Het privacyteam is verantwoordelijk voor het bijhouden van het verwerkingsregister, maar heeft hierbij ook jouw hulp nodig. Indien er een proces verandert, meld dit dan zo snel mogelijk bij het privacyteam. Het is daarnaast ook mogelijk dat een Privacy Officer bij jou op de lijn komt om een bepaalde verwerking te bespreken.

Mag ik persoonsgegevens delen met externe partijen?

Het IMG is bevoegd om gegevens met andere partijen te delen, dit komt omdat het IMG hier een wettelijke grondslag voor heeft. Zo deelt het IMG onder andere gegevens op basis van de grondslag taak van algemeen belang met het college van burgemeester en wethouders van de betrokken gemeentes. Het IMG heeft onder andere met het NCG een gegevensuitwisselingsovereenkomst (GUO) afgesloten. Naast een GUO sluit het IMG ook verwerkersovereenkomsten af met partijen waarmee persoonsgegevens worden gedeeld. Hierin is er vaak sprake van een verwerkingsverantwoordelijke-verwerkers relatie. Indien er twijfels ontstaan over het delen van persoonsgegevens met externe partijen, vraag dan eerst het privacyteam voordat je gegevens deelt met deze partijen.

Wat moet ik doen als ik per ongeluk persoonsgegevens met de verkeerde persoon deel?

Wanneer persoonsgegevens in handen komen van iemand die daar geen toegang toe behoort te hebben, is er sprake van een datalek. Het is menselijk om fouten te maken, maar het is wel zaak om dit zo snel mogelijk te melden bij het privacyteam. Dit heeft te maken met de termijn die door de AP wordt gesteld voor het melden van een datalek, dit is namelijk (72) uur na het ontdekken van het datalek. Het is van belang om snel actie te ondernemen om de schade te beperken. Zodra er bijvoorbeeld per ongeluk een verkeerd bestand aan een dossier is gekoppeld, is het belangrijk dit direct te melden bij het privacyteam. Op die manier vergroot je de kans dat de persoon die toegang heeft tot het dossier het bestand nog niet heeft ingezien. Probeer het privacyteam zo gedetailleerd mogelijk op de hoogte te stellen van het datalek, zo kan er een analyse gemaakt worden van de ernst van het lek en kan het datalek zo snel en goed mogelijk verholpen worden. Hierbij een handige stappenplan dat gevolgd kan worden, mocht er een datalek hebben plaatsgevonden door een verkeerde koppeling in MIRA:

1. Stuur een e-mail naar privacyteam en functioneel beheer met een omschrijving van de volgende punten:
 - o geef aan om wat voor soort document het gaat. Gaat het om iets anders dan een 'standaard' adviesrapport of beslissing, probeer dan kort aan te geven wat de inhoud is en geef aan of het document (bijzondere) persoonsgegevens bevat;
 - o geef aan wanneer het document verstuurd of gekoppeld is;
 - o geef aan wanneer de inbreuk (datalek) plaatsvond;
 - o geef aan wie de ontvanger is, inclusief dossiernummer (BAS of MIRA);
 - o geef aan wie de betrokkene is, en van welk dossier het document onderdeel is, inclusief dossiernummer;

- indien bekend: Geef aan of het document verstuurd is door ons (Serviceloket/AOS afdeling) of door de drukker (Xerox).
- 2. Neem contact op met de ontvanger. Bedank hem/haar voor het doen van de melding, en verzoek om het document ofwel naar ons terug te sturen, ofwel te vernietigen.

Wat zijn voorbeelden van datalekken?

Een datalek kan op verschillende manieren ontstaan. Verschillende voorbeelden van datalekken binnen het IMG zijn:

- het verkeerd koppelen van een document aan een dossier;
- het laten slingeren van documenten met persoonsgegevens bij een printstraat;
- het laten liggen van een USB-stick in een vergaderruimte;
- het onbedoeld versturen van een e-mail met persoonsgegevens naar een derde.

Dit zijn situaties die voor kunnen komen bij het IMG, maar er zijn nog talloze manieren hoe een datalek kan ontstaan. Het is dus goed om door te hebben wanneer er persoonsgegevens in 'verkeerde' handen vallen. Een datalek kan vervelende gevolgen hebben voor de persoon waarvan de gegevens worden verwerkt, denk hierbij bijvoorbeeld aan identiteitsfraude of reputatieschade.

Ik twijfel of ik een datalek heb veroorzaakt, wat moet ik doen?

Indien je twijfelt of je een datalek hebt veroorzaakt, neem dan gelijk contact op met het privacyteam. We hebben liever dat je tien mogelijke datalekken te veel meldt, dan één te weinig. Het privacyteam neemt de kwestie gelijk in behandeling en stuurt jou een terugkoppeling.

Contact

Wij doen ons best toegankelijk en beschikbaar te zijn voor al jouw vragen of meldingen met betrekking tot privacy. Indien er sprake is van een overtreding, verlies of diefstal van gegevens of indien je verdachte zaken constateert, vragen wij jou hier direct een melding van te maken. Voor dergelijke meldingen en/of vragen kun je het beste de algemene mailbox van het privacyteam mailen, privacy@schadedoormijnbouw.nl.

Indien een privacy- of beveiligingsprobleem actief is binnen onze organisatie, zullen wij dit aan alle medewerkers doorgeven. Hierbij kunnen tips, advies en mogelijk te nemen maatregelen medegedeeld worden. Op deze manier proberen wij de medewerkers up-to-date te houden en actief te betrekken. Dit doen we vooral via PLEK⁴ of rechtstreeks via de mail.

Het Instituut heeft daarnaast nog een FG. De FG heeft een onafhankelijke, toezichthoudende functie binnen het Instituut. Dat betekent dat de FG toeziet op de naleving van de privacywet. Heb je misstanden ontdekt die de privacy van betrokkenen kunnen raken, of blijkt de gang van zaken anders te zijn dan afgesproken? Neem dan contact op met de FG. Let op: de FG signaleert over de AVG. Dit betekent dat de FG in principe niet meewerkt bij de *uitvoering* van privacywerkzaamheden, tenzij dit vanuit zijn rol verplicht is.

Informatiebeveiliging

Denk je dat de privacy van betrokkenen niet wordt aangetast, maar heb je een vraag of opmerking over de beveiliging van de systemen, autorisaties of toegang tot locaties?

Neem dan contact op met het team Informatiebeveiliging via

5.1.21 @schadedoormijnbouw.nl.

⁴ [IMG \(plek.co\)](https://plek.co).

5. Bijlagen

- Bijlage 1 - Begrippen
- Bijlage 2 – Beslisboom persoonsgegevens

5.1 Bijlage 1 – Begrippen

Begrip	Verklaring
Betrokkene	De natuurlijke persoon, wiens gegevens worden verzameld, vastgelegd en verwerkt.
Gegevensbescherming	De bescherming van persoonsgegevens, zoals bedoeld in de AVG.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Privacy	We kennen vier vormen van privacy: • Informatieprivacy: gaat over het verwerken en verzamelen van persoonlijke data, bijvoorbeeld financiële gegevens, medische gegevens, contactgegevens etc. • Territoriale privacy: gaat over de persoonlijke omgeving van een individu en de grenzen die hierbij horen, bijvoorbeeld op werk, thuis en publieke ruimtes • Lichamelijke privacy: gaat over de fysieke privacy van een persoon bijvoorbeeld genetische onderzoeken, drugstests, abortus etc. • Communicatieve privacy: gaat over de vrijheden rondom correspondentie via post, telefoongesprekken, e-mail etc.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen

voor de verwerking van persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

5.2 Bijlage 1 – Beslisboom persoonsgegevens

Voor vragen over dit stroomschema: neem contact op met het privacyteam via privacy@schadedoormiinbouw.nl





Werkinstructie voor het blurren van persoonsgegevens

Instituut Mijnbouwschade Groningen (het
Instituut)

Eigenaar: 5.1.2e

Datum : 4 december 2024
Versie : D 1.0
Status : definitief

Colofon

Projectnaam	Werkinstructie voor het blurren van persoonsgegevens
Contactpersoon	5.1.2e Instituut Mijnbouwschade Cascadeplein 10 9726 AD Groningen
Auteurs	5.1.2e
Versie	D 1.0
Bijlage(n)	1

Versie	Datum	Door	Wijzigingen
C 0.1	17-5-2023	5.1.2e	Concept opstel werkwijze
C 0.2	24-6-2023	5.1.2e	Concept bijgewerkt
C 0.3	31-7-2023	5.1.2e	Concept bijgewerkt
C 0.4	14-9-2023	5.1.2e	Concept bijgewerkt
C 0.5	28-9-2023	5.1.2e	Concept bijgewerkt
C 0.6	9-10-2023	5.1.2e &	Concept bijgewerkt
D 1.0	9-10-2023	5.1.2e	Vastgesteld

Inhoudsopgave

1. Inleiding.....	4
1.1 Aanleiding en doel.....	4
1.2 Scope	4
1.3 Contact met privacyteam	4
1.4 Leeswijzer.....	4
1.4 Relevante definities.....	5
2. Werkwijze blurren van persoonsgegevens.....	6
2.1 Instructie voor deskundigen en veldwerk t.a.v. gegevensbescherming.....	6
2.2 Blurren bij datadeling met de NCG en andere externe partijen.....	7
2.3. Blurren van persoonsgegevens in schadehistorie.....	8
2.4. Blurren van persoonsgegevens van overleden personen.....	8
2.5. Blurren bij de regelingen Immateriële schade en Immateriële schade voor het kind en jongere	8
3. Praktische toepassing blurren.....	8
3.1 Online blurren	8
3.2 Blurren van fysieke stukken	9
Bijlage 1: Overzicht persoonsgegevens	10

1. Inleiding

In dit hoofdstuk worden de aanleiding en het doel, de scope, de leeswijzer en de relevante definities van deze werkinstructie omschreven.

1.1 Aanleiding en doel

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG) van toepassing die voor de versterking van privacyrechten van het individu in de huidige digitale wereld heeft gezorgd en daarnaast voor een toename van verantwoordelijkheden voor organisaties. Bij elke verwerking van persoonsgegevens (zie [paragraaf 1.4](#)) dient een organisatie zoals het Instituut Mijnbouwschade Groningen (hierna: het Instituut) zich te houden aan enkele basisprincipes.

Zo vereist de AVG onder andere dat een organisatie passende technische en organisatorische maatregelen moet treffen om persoonsgegevens te beschermen (art. 32 AVG). Ook moet aantoonbaar zijn dat een passende beveiliging gewaarborgd is, zodat betrokkenen beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking (art. 5 AVG).¹

Er komen binnen de organisatie van het Instituut steeds vaker verzoeken binnen, waarbij een derde graag stukken wilt ontvangen waarin persoonsgegevens van een ander staan. Dit leidt tot vragen wanneer er bepaalde stukken mogen worden gedeeld en hoe er moet worden omgegaan met de persoonsgegevens die in deze stukken staan.

Vaak heeft een verzoeker een gerechtvaardigd belang om een bepaald stuk in te zien (denk aan de schadehistorie bij de constatering van eerder behandelde schades). Ook zijn er gevallen bekend waarbij een betrokkene te veel (bijzondere) persoonsgegevens aanlevert in een bepaald document. Voor dit soort situaties kan het blurren van persoonsgegevens de uitgelezen optie zijn. Blurren is het onleesbaar, wazig of onzichtbaar maken van (bepaalde) persoonsgegevens in een (digitaal) bestand met behulp van een computer (-programma) of handmatig, bijvoorbeeld met een zwarte stift. Indien er wordt geblurd, dient het geblurde object volledig onherkenbaar te zijn. Dit betreft een passende technische maatregel in de zin van artikel 32 AVG.

1.2 Scope

Deze werkwijze is bedoeld om inzichtelijk te maken wanneer en hoe blurren moet worden toegepast.

1.3 Contact met privacyteam

Bij twijfel over het wel of niet blurren van bepaalde gegevens kan er contact opgenomen worden met het privacyteam via privacy@schadedoormijnbouw.nl.

1.4 Leeswijzer

In hoofdstuk 2 wordt in een stapsgewijze instructie omschreven in welke situaties het blurren van persoonsgegevens noodzakelijk is. Aan de hand van voorbeelden wordt dit verder geïllustreerd. In hoofdstuk 3 wordt een praktische uitwerking voor blurren uiteengezet. In bijlage 1 treft men een overzicht van persoonsgegevens aan die kan worden gebruikt als legenda bij het blurren.

¹ Persoonsgegevens moeten: door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).

1.4 Relevante definities

Betrokkene	De natuurlijk persoon, wiens gegevens worden verzameld, vastgelegd en verwerkt.
Bijzondere Persoonsgegevens	Bijzondere persoonsgegevens (art. 9 AVG); zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
Blurren	Blurren is niets anders dan een (digitaal) bestand of delen daarvan, wazig of onzichtbaar maken met behulp van een computer (-programma) of handmatig met een zwarte stift. In enkele gevallen kan het voorkomen dat het Instituut iets per post opstuurt, waarbij fysiek blurren met zwarte stift ook mogelijk is.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

2. Werkwijze blurren van persoonsgegevens

In dit hoofdstuk zal er per situatie omschreven worden wanneer en hoe het blurren van persoonsgegevens moet worden toegepast.

2.1 Instructie voor deskundigen en veldwerk t.a.v. gegevensbescherming

Bij de opmaak van adviesrapporten wordt gemerkt dat vele foto's gemaakt door de deskundigen vaak niet voldoen aan de huidige manier van toetsing aan de AVG. Dit houdt in dat veel foto's ter aanpassing terug worden gestuurd naar de deskundige, wat ten koste gaat van de voortvarendheid van de schadeafhandeling.

Het Instituut wil met deze instructie ervoor zorgen dat tijdens de schadeopname de gemaakte foto's zoveel mogelijk al voldoen aan de eisen van de AVG, zodat een uitgebreide controle naderhand achterwege kan blijven. Het doel van deze instructie is dan ook om de deskundigen te voorzien van voldoende handvatten om hun werk naar behoren te kunnen uitvoeren.

Daarbij is geprobeerd om een evenwicht te vinden tussen de verplichting om de verwerking van bijzondere persoonsgegevens zoveel mogelijk tegen te gaan en de wens om de voortvarendheid van de afhandeling niet te belemmeren. Dit neemt niet weg dat deskundigen deels zelf een afweging dienen te maken of het 'blurren' van een foto wel of niet noodzakelijk is. Daarbij doen wij dan ook mede een beroep op het gezonde verstand van de deskundigen.

Deskundigen kunnen tijdens de schadeopname met hun mobiele apparaten (tablet of telefoon) via de Atabix app foto's maken en op deze foto's daar waar nodig de persoonsgegevens onherkenbaar maken (blurren).

Bij het maken van foto's voor een schadeopname dient de deskundige het volgende in acht te nemen:

- Objecten met persoonsgegevens dienen zoveel mogelijk met toestemming van de aanvrager/bewoner te worden weggehaald of buiten het beeld van de foto te worden gehouden;
- Objecten met persoonsgegevens die niet kunnen worden weggehaald of buiten het beeld van de foto kunnen worden gehouden, dienen te worden geblurd;
- Bijzondere persoonsgegevens (zie bijlage I) dienen **altijd** te worden geblurd. Bij het doen van een fysieke schadeopname is het verwerken van bijzondere persoonsgegevens immers niet relevant;
- Overige persoonsgegevens die niet noodzakelijk zijn voor het doel van de verwerking dienen eveneens altijd geblurd te worden.

Daarbij gaat het om de volgende typen objecten:

- Duidelijk herkenbare personen;
- Fotolijsten, portretten, of schilderijen met daarop duidelijk herkenbare personen;
- Religieuze tekenen en symbolen;
- Posters, plakaten en foto's waaruit politieke opvattingen of lidmaatschap van een vakbond blijkt;
- Gegevens over iemand gezondheid (medicijnadoosjes, een brief, etc.);
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.²

Daarbij gelden de volgende aanwijzingen:

Foto's

- 'Duidelijk herkenbaar' houdt in dat de persoon zodanig in beeld is dat het gezicht duidelijk in beeld is, op zo'n manier dat de persoon gemakkelijk zou kunnen worden herkend.
- Gezichten die op de achtergrond staan, onscherp zijn, weggedraaid zijn, of zodanig klein zijn afgebeeld dat deze slechts deels of matig zichtbaar zijn, hoeven niet te worden geblurd.
- Personen die zichtbaar zijn in de reflectie van ramen hoeven niet te worden geblurd, tenzij deze bijzonder goed en van dichtbij zichtbaar zijn.
- Foto's en posters van beroemdheden, bands, TV-sterren, etc. hoeven niet te worden geblurd.

Religieuze symbolen

² Religieuze tekenen, politieke opvattingen, lidmaatschap van een vakbond of iemands seksuele oriëntatie kunnen bijzondere persoonsgegevens zijn en dienen uit voorzorg geblurd te worden (zie ook bijlage I).

- Bij religieuze symbolen en/of tekenen moet er vooral rekening gehouden worden met objecten die redelijkerwijs waarschijnlijk wel iets zullen zeggen over de overtuiging van de aanvrager. Context is daarbij van belang. Een Bijbel, Koran, Torah of ander heilig boek dat op een nachtkastje wordt aangetroffen, zal bijvoorbeeld moeten worden geblurd.
- Hetzelfde geldt voor een kruis, davidsster, etc. aan de muur.
- Bij een enkel los schilderij of beeld met een religieuze context, geldt dat dit geen gegevens zijn, die ook verwerkt dienen te worden in het kader van de schadeopname. Derhalve dienen dit soort gegevens ook geblurd te worden.

Vakbonden en politieke voorkeur

- Posters, plakaten en andere objecten waaruit duidelijk een politieke voorkeur blijkt, dienen te worden geblurd. Dit zijn bijvoorbeeld verkiezingsposters of portretten van politieke leiders.
- Posters, plakaten en andere objecten waaruit lidmaatschap of sterke onderschrijving van een vakbond (bijv. FNV of CNV) blijkt, dienen te worden geblurd.
- Afbeeldingen van leden van het koninklijk huis hoeven niet te worden geblurd.

Seksuele gerichtheid

- Hierbij valt te denken aan LHBT-vlaggen en/of symbolen. Dit zijn gegevens die niet noodzakelijk zijn voor de verwerking en kunnen tevens onder omstandigheden bijzondere persoonsgegevens zijn. Derhalve dienen dit soort gegevens altijd te worden geblurd.
- Zorg ervoor dat de vlag onherkenbaar is op de foto's: enkel blurren zal vaak niet genoeg zijn omdat de kleuren herkenbaar blijven. Plaats over foto's en vlaggen bijvoorbeeld een zwart vlak.

Overig

- Kentekens kunnen worden aangemerkt als een persoonsgegeven en dienen te worden geblurd.
- Denk erom dat er geen documenten zichtbaar op een tafel of bureau liggen waarop mogelijk persoonsgegevens staan afgebeeld, zoals adressen en telefoonnummers. Te denken valt aan facturen, rekeningen, bankafschriften en andere persoonlijke documenten. In geval deze leesbaar worden aangetroffen op de foto's, dienen deze te worden geblurd. Nog beter is het echter wanneer deze bij de schadeopname buiten het zicht worden gelegd.

Op verzoek van aanvrager

- Het kan zijn dat een aanvrager er zelf om verzoekt één of meerdere foto's te blurren, ondanks dat onze eigen werkwijze hier geen aanleiding toe geeft. In die gevallen dient men zoveel mogelijk rekening te houden met de wensen van aanvrager, voor zover dit geen belemmering vormt voor een goede opname van de schade. Hiermee kunnen immers eventuele klachten en andere procedures worden voorkomen.

2.2 Blurren bij datadeling met de NCG en andere externe partijen

Er bestaat tegenwoordig steeds meer behoefte aan samenwerking tussen het Instituut en de Nationaal Coördinator Groningen (hierna: NCG). Sinds juli 2023 bestaat er een uitgebreide wettelijke grondslag om gegevens onderling te delen. Het Instituut en NCG kunnen op eigen beweging en desgevraagd gegevens met elkaar uitwisselen in het kader van de gezamenlijke aanpak conform artikel 3 lid 5 Tijdelijke wet Groningen en het Besluit Tijdelijke wet Groningen, artikel 10h e.v. Er bestaan in het kader van deze integrale aanpak vier fases die worden gespecificeerd in het Besluit Tijdelijke wet Groningen, namelijk: 1) signalering van samenloop; 2) gecoördineerde behandeling; 3) gelijktijdige opname en; 4) integrale uitvoering van schadeherstel en versterking. Vanaf fase 2 dient er toestemming te zijn van de bewoner om gegevens met elkaar uit te wisselen ten behoeve van die fase. Voor de verstrekking van deze gegevens onderling dient ook te worden voldaan de vereisten van de AVG, maar de bespreking van die voorwaarden wordt voor deze werkwijze buiten beschouwing gelaten.

Onderstaand de werkwijze voor het blurren van documenten tussen het IMG en NCG (partijen) en met externe partijen (deskundigen).

Blurren:

- Persoonsgegevens (zie hiervoor + bijlage 1) in de uit te wisselen documenten dienen te worden geblurd, tenzij dat zij relevant zijn voor het doel van de verwerking (denk bijvoorbeeld aan de naam van de bewoner en het adres bij de signalering van samenloop). Het Instituut zorgt ervoor dat de -niet relevante- persoonsgegevens van de bewoner worden geblurd. Het Instituut dient goed te controleren of de niet relevante persoonsgegevens niet zichtbaar zijn.

- In principe worden er enkel en alleen documenten van de huidige bewoner verstrekt aan de ontvangende partij. Indien documenten van een oud bewoner noodzakelijk zijn voor de gezamenlijke aanpak van herstel en versterking (bijvoorbeeld een oud adviesrapport), dan worden de niet relevante persoonsgegevens van de oud bewoner geblurd.

2.3. Blurren van persoonsgegevens in schadehistorie

Bij het Instituut bestaat de mogelijkheid om schadehistorie op te vragen van een object (woning), indien er na een opname door de deskundige wordt geconstateerd dat er sprake is van eerder behandelde schade. Schadehistorie betreft onder andere oude NAM-rapportages en een opnameverslag van het CVW. In deze rapportages kunnen zich persoonsgegevens voordoen door middel van foto's, namen, adressen, burgerservicenummers, etc. van andere personen (oud-aanvragers, deskundigen etc.). Deze persoonsgegevens dienen te worden geblurd.

2.4. Blurren van persoonsgegevens van overleden personen

In principe is het blurren van persoonsgegevens niet noodzakelijk bij overleden personen. De bescherming van persoonsgegevens betreft namelijk alleen natuurlijke personen. Dat houdt in dat het een levend persoon moet betreffen. Toch is het bij het verstrekken van documenten wenselijk om in bepaalde gevallen de gegevens van de overleden persoon te blurren. Stel dat iemand een SNN-subsidie wil aanvragen voor zijn woning en de oud bewoner is overleden. De aanvrager van de SNN-subsidie heeft alleen de informatie nodig dat 1) er een toekenning van schadevergoeding 2) die boven de € 1000,00 is uitgevallen. De overige informatie uit een besluitbrief kan dan achterwege worden gelaten. Deze informatie dient dan ook geblurd te worden. Het kan immers lastig zijn om vast te stellen of de betreffende overleden persoon is overleden. Bovendien is het uit respect voor de overleden persoon en zijn nabestaanden passender om deze informatie niet te delen.

2.5. Blurren bij de regelingen Immateriële schade en Immateriële schade voor het kind en jongere

Bij de regelingen Immateriële schade kunnen er (bijzondere) persoonsgegevens worden aangeleverd, die niet noodzakelijk zijn om de vergoeding van immateriële schade vast te stellen van de aanvrager en/of het kind of de jongere. Deze gegevens dienen in eerste instantie te worden verwijderd door een verzoek te doen bij Functioneel Beheer. Is dat geen mogelijkheid dan dienen deze niet voor de verwerking noodzakelijke persoonsgegevens **altijd** geblurd te worden, mede gelet op het gevoelige karakter van de bijzondere persoonsgegevens.

In het hiernavolgende wordt kort uiteengezet hoe je in de praktijk blurt via Adobe Pro in documenten.

3. Praktische toepassing blurren

3.1 Online blurren

In het hiernavolgende wordt kort uiteengezet hoe je in de praktijk blurt via Adobe Pro in documenten en hoe je documenten handmatig blurt.

Adobe Pro

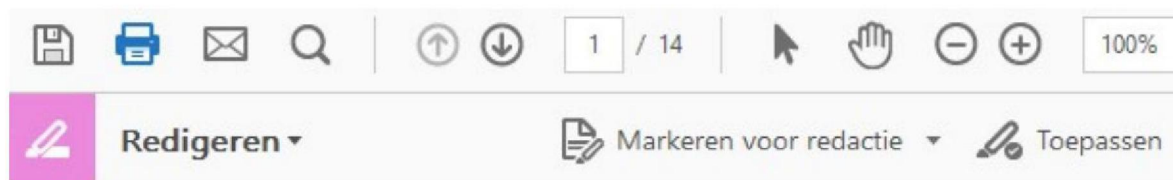
Met Adobe Pro kunnen pdf documenten worden bewerkt.

1. Open Adobe Pro
2. Open het document Bestand > Open. Nu kun je tekst blurren waar nodig.

Wel blurren: persoonsgegevens volgens AVG (zie bijlage 1)

Niet blurren: schadebedragen (dit zijn geen persoonsgegevens). *Het gaat bij het blurren in principe om het verwijderen van persoonsgegevens uit het rapport, de schadebedragen vallen hier niet onder.*

3. Klik op Redigeren
4. Klik op Markeren voor redactie > Tekst en afbeeldingen
5. Klik op Toepassen



Er wordt automatisch een nieuwe bestandsnaam aangemaakt met daarin 'geredigeerd'.

NB: Binnen het Instituut wordt er gezocht naar een innovatievere manier van blurren. Meerdere afdelingen zijn in gesprek met bepaalde partijen om een nieuwe "tooling" aan te schaffen. Indien deze "tooling" wordt aangeschaft, zal deze werkwijze n.a.v. deze "tooling" worden geactualiseerd.

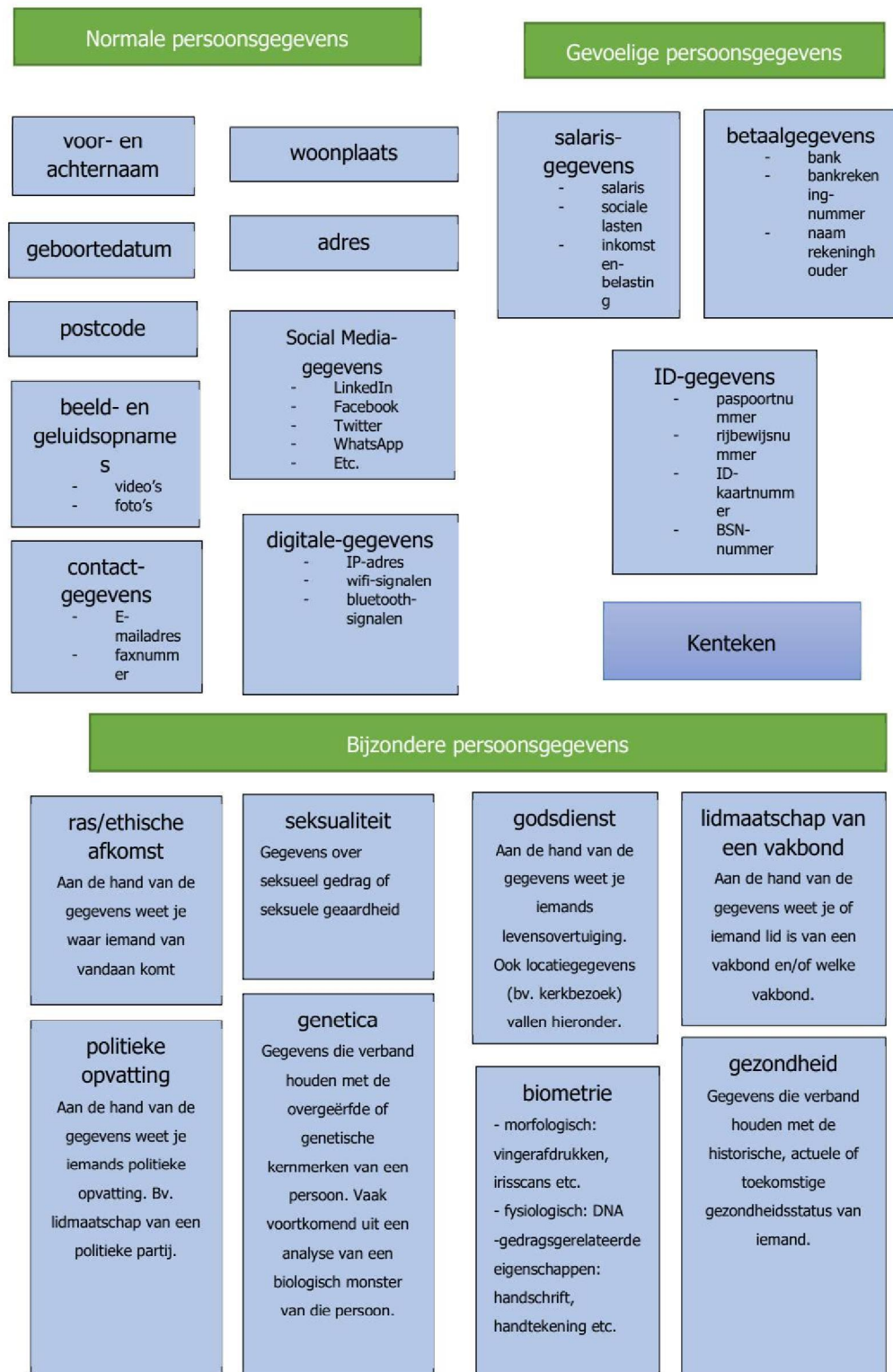
3.2 Blurren van fysieke stukken

Het blurren van persoonsgegevens in fysieke stukken is bovendien ook van groot belang. Dit dient te gebeuren met bijvoorbeeld een zwarte stift.

Wel blurren: persoonsgegevens volgens AVG (zie bijlage 1)

Niet blurren: schadebedragen (dit zijn geen persoonsgegevens). *Het gaat bij het blurren in principe om het verwijderen van persoonsgegevens uit het rapport, de schadebedragen vallen hier niet onder.*

Bijlage 1: Overzicht persoonsgegevens



Uitgangspunten testen met persoonsgegevens:

1. Binnen het Instituut testen we **nooit** met bijzondere persoonsgegevens;
2. Binnen het Instituut testen we, indien mogelijk, met synthetische data of anonieme data;
3. Het verwerkingsdoeleinde voor testen met persoonsgegevens is "het beoordelen en evalueren van een informatiesysteem om de kwaliteit, functionaliteit, betrouwbaarheid en de beveiliging ervan te verifiëren."

Stroomschema testen met persoonsgegevens



*De ontwikkelmethode is van belang voor de frequentie waarmee tests moeten worden uitgevoerd. Agile-ontwikkeling is een voortdurend proces. De afweging of het gebruik van persoonsgegevens voor het uitvoeren van tests gerechtvaardigd is moet periodiek (tenminste eens per jaar) herhaald worden.

**Toets de verenigbaarheid van het doeleinde aan de hand van de criteria uit artikel 6 lid 4 AVG, te weten:

- a) Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en het doeleinde voor testen met persoonsgegevens;
- b) Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen (bijvoorbeeld schadeaanvragers) en het Instituut betreft;
- c) De aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens of strafrechtelijke persoonsgegevens worden verwerkt;
- d) De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen (bijvoorbeeld schadeaanvragers);
- e) Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

***Het gaat hier om beveiligingsvoorwaarden die volgen uit de volgende bronnen:

- a) De ISO norm 27002:2022 geldt als uitgangspunt (zie beleid); daarnaast
- b) Baseline Informatiebeveiliging Overheid (voornamelijk hoofdstuk 14);
- c) Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie; en
- d) Algemene verordening gegevensbescherming.

****Implementatieprocedure:

1. Vraag de CISO en Team Privacy om advies ten aanzien van de gedocumenteerde uitwerking van het toetsingskader en de risicoanalyse;
2. In geval van een test op een applicatie met een dermate hoog of politiek bestuurlijk gevoelig risicoprofiel wordt de Functionaris Gegevensbescherming geraadpleegd;
3. Na positief advies CISO en Team Privacy: vraag de CIO om vaststelling van de gedocumenteerde uitwerking van het toetsingskader en de risicoanalyse
4. Na vaststelling CIO: documenteer de verwerking in het AVG-register (Team Privacy kan hierbij ondersteunen);
5. Na documentatie: implementeer de genomen maatregelen



Testen met persoonsgegevensbeleid

Instituut Mijnbouwschade Groningen
(het Instituut)

Eigenaar: 5.1.2e

Datum : 30 november 2023
Versie : D 1.0
Status : Definitief

Colofon

Projectnaam Testen met persoonsgegevensbeleid

Contactpersoon 5.1.2e

 Instituut Mijnbouwschade
 Cascadeplein 10 | 9726 AD Groningen

Auteurs 5.1.2e en 5.1.2e

Versie 1.0

Bijlage(n) 1

Versie	Datum	Door	Wijzigingen
C 0.1	14-04-2023	5.1.2e	Concept opstel beleid
C 0.2	22-5-2023	5.1.2e	Concept beleid verder uitgewerkt.
C 0.3	13-6-2023	5.1.2e	Beleid n.a.v feedback aangepast
C 0.4	21-6-2023	5.1.2e	Beleid n.a.v beleid EZK aangepast.
C 0.5	11-8-2023	5.1.2e en 5.1.2e	Stroomschema toegevoegd aan beleid als bijlage en beleid verder gefinaliseerd.
C 0.6	7-9-2023	5.1.2e	Definitief concept vastgesteld.
C 0.7	27-10-2023	5.1.2e	Feedback gegeven
C 0.8	28-11-2023	5.1.2e	Definitief concept voorgelegd aan MT.
D 1.0	30-11-2023	5.1.2e	Vastgesteld

Inhoudsopgave

1. Inleiding	6
1.1 Aanleiding en doel.....	6
1.2 Scope	6
1.3 Leeswijzer.....	6
1.4 Samenhang met aanpalend beleid.....	7
1.5 Relevante definities	7
2. Governance	8
3. Toetsingskader testen met persoonsgegevens	9
3.1 Voorwaarden AVG	9
3.2. Beveiligingsnormen	10
3.3 Overige voorwaarden	11
4. Risicoanalyse, mitigerende maatregelen en risico-acceptatie	12
4.1 Risicoanalyse.....	12
4.2 Mitigerende maatregelen.....	12
4.3 Risico-acceptatie	13
5 Procedure	14
5.1 Procedure schematisch weergegeven.....	14
Bijlage I: Stroomschema testen met persoonsgegevens	15

1. Inleiding

1.1 Aanleiding en doel

Binnen het Instituut Mijnbouwschade Groningen (hierna: het Instituut) bestaat de wens om te testen met persoonsgegevens. Bepaalde organisatieonderdelen willen de bedrijfsvoering verbeteren en ondersteunen door middel van het uitvoeren van bepaalde testen en daarmee is het noodzakelijk om bij sommige tests persoonsgegevens worden gebruikt.

Zowel systeemtesten als acceptatietesten vereisen gewoonlijk substantiële hoeveelheden testgegevens die een zo getrouw mogelijke weergave moeten zijn van productiedata. Ook het gebruik van nieuwe analyse methoden om datagedreven te werken vereist een enorme hoeveel aan productiedata. Door het gebruik van productiedata voor het testen kunnen echter de vertrouwelijkheid en privacy van aanvragers geschonden worden. Het verwerken van persoonsgegevens voor testdoeleinden wordt daarom aan strenge wettelijke vereisten getoetst. Uitgangspunt van het Instituut is dat het testen met persoonsgegevens altijd in lijn moet zijn met die wettelijke vereisten. Het onzorgvuldig omgaan met het testen van persoonsgegevens kan immers leiden tot datalekken en gegevens kunnen ongewild in het primaire proces terecht komen, waardoor bijvoorbeeld burgers foutieve informatie ontvangen of andere schadelijke gevolgen ondervinden.

De Algemene verordening gegevensbescherming (hierna: AVG) vereist van organisaties dat elke verwerking van persoonsgegevens voldoet aan een aantal basisprincipes in de zin van artikel 5 en 6 AVG. Zo moet er voor elke verwerking een wettelijke grondslag bestaan om persoonsgegevens te verwerken. Het verwerken van persoonsgegevens voor testdoeleinden is een verwerking in de zin van artikel 2 lid 1 AVG jo. 4 lid 1 en 2 AVG.

De persoonsgegevens zijn bij het Instituut vaak verzameld voor een ander doel dan testen, in de meeste gevallen het afhandelen van een aanvraag tot schadevergoeding. Daarom mag er niet zomaar worden getest met persoonsgegevens, want dit zou een verwerking voor een ander doel behelzen die ook een andere verwerkingsgrondslag behoeft. Vooropgesteld wordt het testen met persoonsgegevens afgeraden door de Autoriteit Persoonsgegevens (hierna: AP) en het Instituut schaaft zich hierachter.¹ Het gebruik van synthetische data / anonieme data heeft daarom altijd de voorkeur. Tegelijkertijd beseft het Instituut zich goed dat het verwerken van persoonsgegevens voor testdoeleinden soms noodzakelijk kan zijn. De AVG kan ruimte bieden om in sommige gevallen met persoonsgegevens te testen.

Dit beleid heeft als uitgangspunt dat het wordt afgeraden om persoonsgegevens te verwerken voor testdoeleinden. In de gevallen dat er voor het testen geen synthetische of anonieme data kan worden gebruikt en het verwerken van persoonsgegevens echt noodzakelijk is, dient onderstaand beleid te worden gevolgd. De uitgangspunten met betrekking tot het verwerken van persoonsgegevens voor testdoeleinden van het Ministerie van Economische Zaken en Klimaat zijn in dit beleid verwerkt.

1.2 Scope

Dit beleid geldt voor alle teams die zowel intern werken voor het Instituut als de teams die in opdracht van het Instituut persoonsgegevens willen verwerken voor testdoeleinden ten behoeve van het primaire proces of secundaire proces van het Instituut.

Dit beleid is van toepassing op alle onderdelen/afdelingen van het Instituut.

1.3 Leeswijzer

In hoofdstuk 2 wordt de governance beschreven. Vervolgens wordt er in hoofdstuk 3 het toetsingskader beschreven voor het testen met persoonsgegevens. In hoofdstuk 4 wordt besproken hoe er een risicoanalyse dient te worden gehouden indien aan de vereisen van hoofdstuk 2 wordt voldaan. In hoofdstuk 5 wordt tot slot besproken hoe de procedure werkt voor het testen met persoonsgegevens. In bijlage 1 wordt dit beleid op een praktische wijze in de vorm van een stroomschema weergegeven.

¹ [Beveiliging van persoonsgegevens | Autoriteit Persoonsgegevens](#)

1.4 Samenhang met aanpalend beleid

Dit beleidsdocument moet gelezen en begrepen worden in samenhang met diverse andere beleidsstukken. Van het Instituut zelf zijn dat de volgende documenten:

- Privacybeleid IMG;²
- Logging en monitoring beleid IMG;³ en
- Strategische Informatiebeveiligingsbeleid.⁴

Deze beleidstukken (van diverse overheidsinstanties) zijn eveneens relevant:

- Voorschrift Informatiebeveiliging Rijksdienst (VIR); en
- Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI) en;
- Testen met productiedata EZK en LNV.⁵

1.5 Relevante definities

In deze paragraaf treft men de relevante begrippen aan die van belang zijn voor dit document:

Acceptatietesten	Testen die zijn bedoeld om te bepalen of het systeem voldoet aan de vereisten en verwachtingen van de eindgebruikers, klanten of belanghebbenden. Deze tests worden uitgevoerd nadat de systeemtesten zijn voltooid en eventuele belangrijke problemen zijn opgelost.
Fictieve of gegenereerde data	Gegevens die zelf gecreëerd zijn en op geen enkele wijze verwijzen naar (gevoelige) gegevens vanuit productie (omgeving).
Geanonimiseerde gegevens	Gegevens die niet langer kunnen worden herleid tot individuen, zelfs niet door het combineren met andere gegevens of geavanceerde technieken.
Gepseudonimiseerde persoonsgegevens	Persoonsgegevens die niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt. Deze aanvullende gegevens dienen apart te worden bewaard en er dienen maatregelen te worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. ⁶
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer,

² 5.1.2e 'Privacybeleid IMG,' versie 1, 1 februari 2022.

³ 5.1.2e 'Logging en monitoringsbeleid Instituut Mijnbouwschade Groningen (IMG),' versie 1, 22 juli 2021.

⁴ 5.1.2e 'Informatiebeveiligingsbeleid Instituut Mijnbouwschade Groningen', versie 1.01, 4 november 2021.

⁵ 5.1.2e en 5.1.2e 'Testen met productiedata EZK en LNV, versie c.1.0, 19 juni 2023.

⁶ Artikel 4 EU algemene verordening gegevensbescherming (EU-AVG). [Privacy/Privazy according to plan. \(privacy-regulation.eu\)](#)

	locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Productiedata (of besturingsinformatie)	Gegevens of delen daarvan die daadwerkelijk in het primaire proces of secundaire proces gebruikt of verwerkt worden. ⁷
Systeemtesten	Deze testen zijn gericht op het testen van het volledige geïntegreerde systeem om te controleren of het voldoet aan de functionele en technische specificaties. Deze tests worden uitgevoerd nadat de afzonderlijke componenten of modules van het systeem zijn ontwikkeld en getest. Het doel is om eventuele systeemfouten, bugs of inconsistenties te identificeren voordat het systeem in gebruik wordt genomen.
Tekstmining	Een overkoepelende term die verwijst naar het proces om met allerlei technieken waardevolle informatie te halen uit grote hoeveelheden tekstmateriaal. Met deze technieken wordt gepoogd patronen en tendensen te ontwaren. Concreet gaat men teksten softwarematig structureren en ontleden, transformeren, vervolgens inbrengen in databanken, en ten slotte evalueren en interpreteren.
Testen	Het proces van het beoordelen en evalueren van een informatiesysteem om de kwaliteit, functionaliteit, betrouwbaarheid en de beveiliging ervan te verifiëren.
Verwerken	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

2. Governance

De governance voor dit beleid is ingericht zoals weergegeven in het privacybeleid⁸ van het Instituut.

⁷ Waar de ISO spreekt over operationele gegevens duiden we dat binnen EZK en LNV als productiedata.

⁸ 5.1.2e 'Privacybeleid IMG,' versie 1, 1 februari 2022.

3. Toetsingskader testen met persoonsgegevens

Ten eerste heeft het Instituut een aantal uitgangspunten. Voor systeemtesten is het niet toegestaan om persoonsgegevens te verwerken voor testdoeleinden. Het gebruik van dummy of synthetische data is voldoende om een test succesvol te laten zijn en derhalve is het verwerken van persoonsgegevens voor testdoeleinden voor systeemtesten niet noodzakelijk. Het is beginsel niet toegestaan om bijzondere persoonsgegevens te verwerken voor testdoeleinden, tenzij er een wettelijke uitzonderingsgrondslag bestaat die dit toestaat. Voorts moet elke test zowel voldoen aan de Baseline Informatiebeveiliging Overheid (hierna: BIO) als aan de AVG en aan (toekomstige) aanverwante wetgeving.

Er mag in beginsel alleen productiedata gebruikt worden voor testdoeleinden, indien de volgende voorstappen worden genomen. Door het gebruik van productiedata voor testen kunnen de vertrouwelijkheid en privacy geschonden worden. Daarom is het testen met productiedata in principe alleen toegestaan, indien er gebruik wordt gemaakt van anonimiseringstechnieken (waardoor alle persoonsgegevens worden geanonimiseerd) dan wel het gebruik van fictieve data. Testen geschiedt derhalve met geanonimiseerde gegevens of met fictieve, gegenereerde data. Bij het (her)ontwerp van systemen en ketens moet rekening worden gehouden met deze principes.

Als voorgaande stappen niet toegepast kunnen worden en het verwerken van persoonsgegevens voor testdoeleinden onvermijdelijk worden geacht, moet aan de voorwaarden uit onderstaande drie paragrafen worden voldaan. Zoals nader toegelicht, wordt de beoordeling of er wordt voldaan aan deze drie voorwaarden altijd uitgevoerd door het team Informatiebeveiliging en Privacy (hierna: IB&P). Wel wordt het projectteam / de tester geadviseerd om onderstaande voorwaarden goed door te nemen, zodat bij het doen van een testvoorstel onderstaande voorwaarden al in acht zijn genomen.

3.1 Voorwaarden AVG

De AVG bevat regels voor de omgang met persoonsgegevens. Uitgangspunt is dat persoonsgegevens alleen verwerkt mogen worden als dat verenigbaar is met het doel waarvoor de gegevens zijn verzameld, de verwerking plaatsvindt op basis van een rechtmatige grondslag én de verwerking proportioneel (minimale gegevensverwerking) en subsidiair (geen minder ingrijpend alternatief) is. Ook de juistheid (integriteit) van persoonsgegevens vormt een integraal onderdeel van de gegevensverwerking.

De grondslag voor het verwerken van persoonsgegevens is essentieel omdat het de wettelijke basis vormt voor het rechtmatig verwerken van persoonsgegevens.

Een grondslag is nodig om ervoor te zorgen dat de verwerking van persoonsgegevens aan bepaalde voorwaarden voldoet en dat de rechten en vrijheden van betrokkenen worden beschermd. Het zorgt ook voor een evenwicht tussen de behoefte aan het verwerken van persoonsgegevens en de bescherming van de privacy van burgers.

De AVG biedt zes verschillende grondslagen voor rechtmatige verwerking van persoonsgegevens. Voor het Instituut zijn vooral de grondslagen wettelijke verplichting en taak van algemeen belang relevant:

- Noodzakelijk ter uitvoering van een wettelijke verplichting: de verwerking is noodzakelijk het voor het uitvoeren van een wettelijke verplichting;
- Taak van algemeen belang of uitoefening van openbaar gezag: de verwerking is noodzakelijk voor de uitoefening van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

Bij het uitvoeren van testen met (gepseudonimiseerde) persoonsgegevens en productiedata is sprake van zogenaamde verdere verwerking, persoonsgegevens worden verwerkt voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk werden verzameld. Art. 6 lid 4 AVG legt uit dat een verder verwerking alleen mogelijk is indien:

De verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld en de verwerkingsverantwoordelijke bij de beoordeling van de verenigbaarheid onder meer rekening houdt met:

- a) Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- b) Het kader waarin de persoonsgegevens zijn verzameld, met name wat betreft de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke;
- c) De aard van de persoonsgegevens, met name of bijzondere categorieën persoonsgegevens worden verwerkt en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt;
- d) De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
- e) Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Het gebruik van persoonsgegevens bij testen kan in sommige gevallen verenigbaar zijn met het oorspronkelijke doel. Bijvoorbeeld het testen van een applicatie voor de uitvoering van een subsidieregeling. Doorloop de stappen uit onder andere art. 6 lid 4 AVG. Is de beoordeling dat de verdere verwerking verenigbaar is met het oorspronkelijke doel? Dan is in dit voorbeeld de grondslag voor het testen van de applicatie dezelfde grondslag als de uitvoering van de subsidieregeling, namelijk het uitvoeren van een taak van algemeen belang.

Kortom, het verder verwerken van persoonsgegevens in een test is soms toegestaan, maar rechtvaardigt niet dat in alle gevallen productiedata wordt gebruikt voor het uitvoeren van tests.

Naast de verenigbaarheidstoets dient ook te worden getoetst of het testen met productiedata proportioneel is en of er alternatieve methoden zijn die de privacy van betrokkenen beter beschermen, zoals het gebruik van geanonimiseerde testgegevens of synthetische testgegevens.

Tevens dienen de volgende beginselen in acht te worden genomen:

1. Er dient een welbepaald, uitdrukkelijk en omschreven doel te zijn voor het testen van persoonsgegevens.
2. Als er getest wordt met persoonsgegevens wordt er alleen getest in een beveiligde omgeving die voldoet aan de BIO (zie paragraaf 2.2).
3. Bij elke test worden er zo weinig mogelijk persoonsgegevens verwerkt. Alleen die gegevens die er nodig zijn om de test te effectueren mogen worden verwerkt.
4. De persoonsgegevens die zijn gebruikt voor het testen worden na de uitvoering van de test per direct verwijderd.
5. Er wordt op voorhand afgestemd met de CISO, het privacyteam en de functionaris gegevensbescherming om te beoordelen of het verwerken van persoonsgegevens voor testdoelen in de gegeven omstandigheden gerechtvaardigd kan zijn (zie hoofdstuk 5).

3.2.Beveiligingsnormen

Wetgeving als de AVG en de Baseline Informatiebeveiliging Overheid (BIO) schrijven voor dat persoonsgegevens op een juiste manier worden beveiligd. Om bijvoorbeeld datalekken te voorkomen moeten overheden passende technische- en organisatorische maatregelen nemen. Voorafgaand aan de verwerking moet worden nagedacht over deze beveiliging. Er dienen moderne technieken te worden toegepast en overheden moeten verder kijken dan de techniek alleen, bijvoorbeeld wie er toegang heeft tot de gegevens. De uitwerking van maatregelen in dit document is een verdere detaillering van onderstaande maatregel uit de BIO.

14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

14.3.1 2 Bescherming van testgegevens Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Proceseigenaar Dienstenleverancier
--	---------------------------------------

Voor de verdere uitwerking van de maatregelen is de ISO norm 27002:2022⁹ als uitgangspunt genomen. In deze norm wordt beschreven hoe testgegevens op passende wijze worden geselecteerd, beschermd en beheerd en stelt het volgende:

Systeem- en acceptatietests vereisen gewoonlijk substantiële hoeveelheden testgegevens die een zo getrouw mogelijke weergave moeten zijn van productiegegevens.

Het voor testdoeleinden gebruiken van productiedatabases met persoonsgegevens of enige andere vertrouwelijke informatie behoort te worden vermeden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoeleinden, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen. De volgende richtlijnen behoren te worden toegepast om operationele gegevens te beschermen die voor testdoeleinden worden gebruikt te beschermen, ongeacht of de testomgeving lokaal is gebouwd of zich op een clouddienst bevindt:

- a) de toegangsbeveiligingsprocedures die worden toegepast op operationele omgevingen, worden ook op testomgevingen toegepast;*
- b) voor elke keer dat productiedata naar een testomgeving wordt gekopieerd, behoort een afzonderlijke autorisatie te worden verkregen;*
- c) van het kopiëren en gebruiken van productiedata behoort verslaglegging te worden bijgehouden om in een audittraject te voorzien;*
- d) gevoelige gegevens worden beschermd door deze te verwijderen of te maskeren bij gebruik voor testen;*
- e) Productiedata behoort onmiddellijk na voltooiing van het testen uit een testomgeving te worden verwijderd.*

3.3 Overige voorwaarden

Naast eerder genoemde wetgeving kan in specifieke situaties ook andere wetgeving van toepassing zijn op testen met productiedata. Het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013) stelt eisen aan informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries (bijzondere informatie). De Wet Bescherming Bedrijfsgeheimen, betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) stelt eisen aan het rechtmatig verkrijgen, gebruiken of openbaar maken van bedrijfsgeheimen. De Wet op het financieel toezicht (Wft) bepaalt dat alle vertrouwelijke gegevens en inlichtingen die door haar toezicht zijn verkregen, geheim zijn. De Wft verstaat onder vertrouwelijke informatie in elk geval concurrentiegevoelige informatie en informatie die een disproportionele inbreuk maakt op de persoonlijke levenssfeer.

Verder is de frequentie waarmee de voorwaarden uit dit hoofdstuk moeten worden herhaald afhankelijk van de softwareontwikkelmethode. Bij de klassieke watervalmethode wordt per project de afweging gemaakt of er extra maatregelen nodig zijn om de verdere verwerking van (bijzondere) persoonsgegevens in de productietestomgeving te rechtvaardigen. Bij de Agile-softwareontwikkeling is er sprake van continue ontwikkeling. De afwegingen moeten daarom periodiek herhaald worden en tenminste eenmaal per jaar. Echter wanneer er bij een Agile-aanpak sprake is van bijzondere persoonsgegevens moeten afwegingen uit dit toetsingskader gemaakt worden voor elke (serie) iteratie(s) waarbij dit het geval is.

Als aan de voorwaarden van hoofdstuk 2 wordt voldaan om met productiedata, waaronder persoonsgegevens, te mogen testen dan moeten de risico's van testen met productiedata in kaart gebracht worden. Als de kans op en/of impact van een verstoring groot is dienen aanvullende maatregelen genomen om de productiedata te beschermen (mitigerende maatregelen).

⁹ ISO 27002:2022 Informatiebeveiliging, cybersecurity en bescherming van de privacy – Beheersmaatregelen voor informatiebeveiliging.

4. Risicoanalyse, mitigerende maatregelen en risico-acceptatie

In dit hoofdstuk wordt het proces van een risicoanalyse omschreven. Eerst dienen er risico's in kaart te worden gebracht en vervolgens moeten er maatregelen worden bedacht om de risico's te mitigeren. Er worden een aantal voorbeelden genoemd van mitigerende maatregelen.

4.1 Risicoanalyse

De risico's van het testen met productiedata moeten in kaart gebracht worden. Het gaat hier om de potentiële ongewenste gevolgen, zoals datalekken en gegevens die ongewild in het primaire proces terecht kunnen komen, waardoor bijvoorbeeld burgers en bedrijven foutieve informatie ontvangen of andere schadelijke gevolgen ondervinden. Deze risico's dienen te worden afgewogen tegen de risico's wanneer er geen test met productiedata wordt uitgevoerd, maar bijvoorbeeld met gegenereerde data.

4.2 Mitigerende maatregelen

Het uitgangspunt is dat als er in een testomgeving productiedata worden opgenomen, de testomgeving aan beveiligingseisen moet voldoen die vergelijkbaar zijn met eisen voor de productieomgeving die voortvloeien uit de VIRBI, AVG, BIO en andere kaders en normen. Dit betekent dat extra maatregelen moeten worden getroffen om de bescherming van de gegevens te waarborgen. In ieder geval moeten onderstaande maatregelen worden genomen, tenzij er (andere) betere maatregelen voor het specifieke geval van toepassing zijn.

Degene die voornemens is om met persoonsgegevens (geldt dus ook voor gepseudonimiseerde gegevens) te testen moet daarvoor de risico's in kaart brengen. Bij hoge risico's of bij specifiek aangegeven situaties die volgen uit het beleid van de Rijksoverheid moet een Data protection impact assessment (DPIA) worden uitgevoerd.¹⁰ Indien er gebruik wordt gemaakt van algoritmes die volgens de AI-verordening in de categorie hoog risico algoritmes vallen of die volgens het beleid van de Rijksoverheid impactvol zijn, kan het uitvoeren van een Impact Assessment Mensenrechten en Algoritmes (IAMA) eveneens een vereiste zijn. Het resultaat van de assessment(s) wordt toegevoegd aan de registratie van de verwerking in het AVG-verwerkingenregister en/of aan de registratie van het algoritme in het Algoritmeregister.

Als het gaat om gegevens van medewerkers vereist het afstemming/instemming met/van de OR (WOR Art. 27j,k).

Acceptatietesten en tekstmining vereisen gewoonlijk substantiële hoeveelheden testgegevens die een zo getrouw mogelijke weergave moeten zijn van productiedata. De 'privacy by design en 'privacy by default' beginselen dienen te worden toegepast door pseudonimisering en/of anonimiseren/minimalisering van de gegevens, bijvoorbeeld alleen salaris relevante gegevens bij het testen van een payrolsysteem, niet naam, geslacht, etc.

De toegang moet beperkt worden door strikte autorisatie toe te passen, ten minste zoals in productie. Beperk de toegang tot personen die normaliter al toegang hebben tot de gegevens.

Voor elke keer dat productiedata naar een testomgeving worden gekopieerd, behoort een afzonderlijke autorisatie te worden verkregen. Gegevens mogen niet online toegankelijk zijn als dat niet noodzakelijk is. De beschikbaarheidsduur van gegevens moet beperkt zijn door pas direct voor de test gegevens beschikbaar te stellen in een acceptatieomgeving en deze direct na afloop van de test te verwijderen (na analyse van eventuele fouten). Eventuele externe partijen die betrokken zijn bij de uitvoering van de test moeten testgegevens ook direct verwijderen na afloop.

De gegevens en systemen moeten afgeschermd zijn van de productieomgeving. Er moeten maatregelen genomen worden om de herkenbaarheid van de testomgeving en gegevens te borgen. Output moet herkenbaar zijn als testoutput op printers en beeldschermen, zodat op het beeldscherm op elk moment herkenbaar is dat het om een testomgeving gaat. (bijv. afwijkende kleur en/of waarschuwing op het scherm/printout).

¹⁰ Zie Rijksmodel DPIA 2022, p. 6.