

objecten zijn in beginsel geen persoonsgegevens. Deze informatie kwalificeert weer wel als persoonsgegevens indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *we* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegevens vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- * ras of etnische afkomst;
- * politieke opvattingen;
- * religieuze of levensbeschouwelijke overtuigingen;
- * het lidmaatschap van een vakbond;
- * genetische gegevens;
- * biometrische gegevens met het oog op de unieke identificatie van een persoon;
- * gegevens over gezondheid;
- * gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie- en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij

aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- b. personen die voor een strafbaar feit zijn veroordeeld;
- c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij conceptregelgeving kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

[Klik hier om infotekst te verbergen](#)

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder

pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie- en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk

gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- personen die voor een strafbaar feit zijn veroordeeld;
- slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij **conceptregelgeving** kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

In Atabix worden verschillende categorieën persoonsgegevens verwerkt, die voor het grootste deel overeenstemmen met de categorieën persoonsgegevens die in het kader van de reguliere procedure voor vergoeding van fysieke schade worden verwerkt.

In onderstaand figuur 1.0 wordt een overzicht van de persoonsgegevens weergegeven. In dit figuur worden de categorieën van persoonsgegevens opgesomd die worden verwerkt. Hierbij wordt aangegeven wie de verstrekker is van de gegevens en op wie het betrekking heeft.

Figuur 1.0

Wie?	Verstrekker	Input - (Persoons)gegevens	Type gegevens
anvrager, Intermediair, deskundigen en gebruikers ¹	DigiD (Logius)	1. IP-adressen aanvrager	1. Gewone persoonsgegevens 2. Wettelijk identificerende gegevens ²
	Relatieservice s RVO – Basisregistrati	1. NAW-gegevens (naam, adres en woongegevens) aanvrager	1. Wettelijk Identificerend 2. Gewone persoonsgegevens

¹ Gebruikers Atabix; onder gebruikers wordt verstaan IMG medewerkers en ontwikkelaars/ beheerders van de software Atabix (Atabix ontwikkelingsteams).

² Het IMG verwerkt het Burgerservicenummer (BSN) van zijn aanvragers bij de aanvraag via DigiD. In Atabix worden de BSN nummers niet verwerkt.

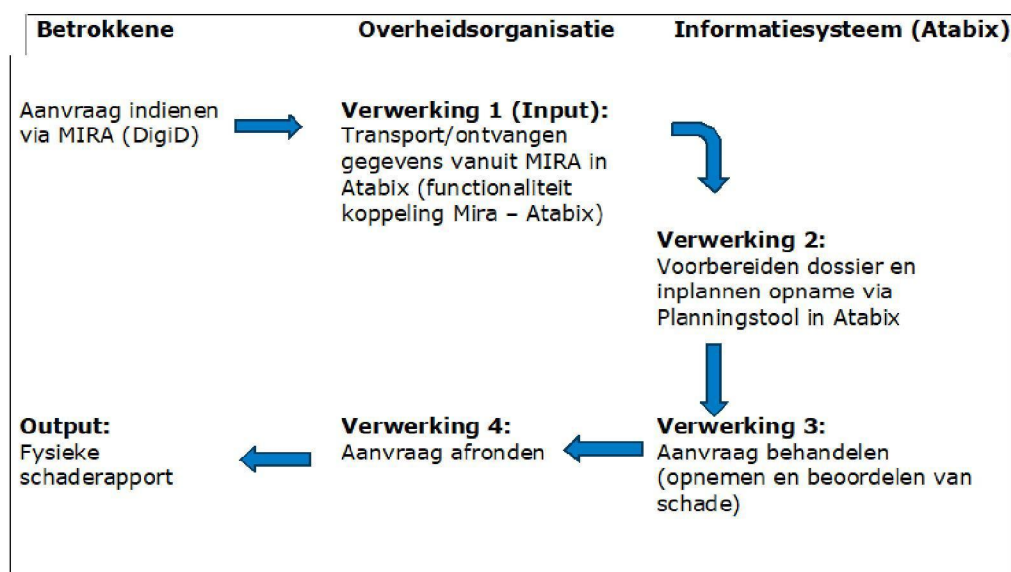
e Personen (BRP) als input voor MIRA.	2. Geboortedatum aanvrager	3. Gewone persoonsgegevens
MIRA (persoonsgegevens van aanvrager en/of intermediair) IMG (fysieke schade zaken)	1. NAW-gegevens (naam, adres en woongegevens) aanvrager 2. Telefoonnummer aanvrager 3. E-mailadres aanvrager 4. Zaakinformatie (zaaknummer, datum melding, datum besluit, vergoeding) 5. Gebouwkenmerken (woningtype, bouwjaar, kwetsbaarheid gebouw, woonbestemming etc.) 6. Start- en einddatum eigendom aanvrager 7.	1. Gewone persoonsgegevens 2. Gewone persoonsgegevens 3. Gewone persoonsgegevens 4. Gewone persoonsgegevens 5. –
Door deskundigen zelf ingegeven	1. Telefoonnummer deskundige 2. E-mailadres deskundige 3. Verbeteringen op eigendomsgegevens zoals bekend bij het Kadaster 4. Bewijsstukken 5. Gebouwkenmerken (woningtype, bouwjaar, kwetsbaarheid gebouw, aantal en welke bouwlagen etc.) 6. Ruimtekenmerken (afwerking, materiaal, oppervlakte, etc.) 7. Schadekenmerken 8. Omgevingskenmerken 9. IP-adressen deskundige 10. Ruimtekenmerken (afwerking, materiaal, oppervlakte, etc.) 11. Schadekenmerken 12. Omgevingskenmerken 13. Foto's van schade pand; op deze afbeeldingen kan nadere informatie zichtbaar zijn, waaronder (bijzondere) persoonsgegevens;	1. Gewone persoonsgegevens 2. Gewone persoonsgegevens 3. Gewone persoonsgegevens 4. Gewone persoonsgegevens (afhankelijk van het bewijsstuk) 5. – 6. – 7. – 8. – 9. Gewone persoonsgegevens 10. – 11. – 12. – 13. Gewone persoonsgegevens, waaronder metadata en mogelijk bijzondere persoonsgegevens
Aanvragers (via Planningstool)	1. Telefoonnummer aanvrager 2. E-mailadres aanvrager	1. Gewone persoonsgegevens 2. Gewone persoonsgegevens
Kadaster	1. Eigendom perceel	1. Gewone persoonsgegevens

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Binnen het IMG maken de volgende organisatie onderdelen (afdelingen) gebruik van Atabix. En daarmee het "verwerken" van persoonsgegevens in Atabix (cf. art. 4 lid 2 AVG).

Gegevensverwerking in Atabix.



Toelichting gegevensverwerking in Atabix:

Alle processen en regelingen, zoals hieronder opgesomd, volgen dit hoofdproces. Er kunnen echter onderlinge verschillen en specificaties zijn, afhankelijk van het proces/de regeling. Daar wordt niet op ingegaan, omdat er afzonderlijke DPIA's zijn/worden opgesteld voor die processen.

- Fysieke schade - schade aan gebouwen en objecten - Regulier proces
- Herstel in Natura (aparte omgeving in Atabix) → vallend onder Schade Expertise & Herstel (SEH)
- VES - vaste vergoeding voor schade aan woningen - Atabix alleen voor de planningstool
- Immateriële schade - Atabix alleen voor de planningstool
- Ambtelijk bezwaar
- Bezwaar

Input (verwerking 1 – indienen en registreren):

De gegevensverwerking in Atabix start vanuit MIRA. Aanvrager/intermediair dient een aanvraag, waarna de gegevens van aanvrager en/of intermediair van MIRA naar Atabix (functionaliteit Koppeling Mira - Atabix) wordt getransporteerd.

Met de koppeling wordt in een Atabix zaak aangemaakt op basis van het dossier – de zaak – in MIRA. Daarbij worden de gegevensgroepen; Eigenaarschap en vertegenwoordiging, Gebouwenmerken, Schadekenmerken en Overige schades meegegeven van MIRA naar Atabix. Bij overdracht van MIRA naar Atabix worden de volgende (persoons)gegevens verwerkt:

- Adres aanvrager/intermediair
- Telefoonnummer aanvrager/intermediair
- E-mailadres aanvrager/intermediair
- Gegevens over de woning en schades:
 - Bouwjaar
 - Speciale status?

- Gebruik woning
- Kadastrale aanduiding (wordt in MIRA opgehaald en gekopieerd naar Atabix)
- Sinds wanneer huidige eigenaar
- Hoeveel schades totaal
- Soort schade
- Wanneer schade is ontstaan
- Omschrijving schade
- BTW-plichtig?

Verwerking 2 (voorbereiden, inplannen en toewijzen deskundige)

De persoonsgegevens van de aanvrager worden bij het voorbereiden van dossier in Atabix gebruikt. Voor opname wordt het dossier klaargemaakt en een opname ingepland. Daarvoor worden de volgende functies behandeld via de **planningstool**.

- Beheren zaakbegeleiders
- Afspraken plannen
- Selecteren zaakbegeleider bij dossier\afspraak
- Beheren agenda's zaakbegeleiders
- Plannen terugbelafspraak
- Afspraken annuleren

Verwerking 3 (Opnemen, calculeren, adviesrapport):

Door het gebruik van diverse tooling in Atabix worden de gegevens van aanvrager inzichtelijk en bewerkbaar. De tooling bij deze verwerking zijn:

- **Opnametool voor deskundigen** (Atabix)
- **Dossier editor** → Het toevoegen (verrijken) van gegevens van aanvrager door medewerkers IMG en externe (deskundigen). D.m.v. de dossierstructuur kunnen verdere gegevens worden opgenomen en gekoppeld aan de persoon.
Deskundigen van verschillende deskundigenbureaus kunnen elkaars dossiers niet inzien.
Binnen deskundigenbureaus hangt het ervan af hoe de deskundigenbureaus dat inrichten.
- De **trillingstool** en **PETAT** (**5.1.2e** en **5.1.2e** **Aardbevings Tool**) worden gebruikt bij aanvragen in Atabix. Deze tools zullen naast de nieuwe GIS tool draaien. De bedoeling bij GIS om deze tooling na te bouwen in eigen omgeving (beheer DICTU). Met de trillingstool / PETAT tool in Atabix, is het mogelijk om zoekend op een adres, naastgelegen dossiers van andere partijen (in .pdf format) in te zien en te downloaden.

Afronding - verwerking 4 (Toetsen, voorbereiden besluit, beoordelen besluit en uitbetalen):

De verwerkte gegevens in Atabix worden als een fysieke schaderapport (output) opgeleverd (via rapport generator) in een pdf-bestand.

Na oplevering van het schaderapport wordt het proces verder voortgezet door de afdeling BJZS (beslisorgaan) om een beslissing (besluit) te nemen op de (eventuele) schade en uit te keren.

Vervolgens wordt het rapport overgezet naar MIRA, waardoor het beschikbaar komt voor de aanvrager.

Twee weken na opmaken van het adviesrapport kan een zienswijze worden ingediend door de aanvrager. Naar aanleiding daarvan kan om nader advies van een deskundige worden gevraagd. Dit verloopt via Atabix.

De genereerde data in Atabix wordt eveneens naar de SAS omgeving (beheer DICTU) oftewel het Datawarehouse (DWH) gezet. De data stroomt van de AWS omgeving van Atabix naar de SAS omgeving van IMG. Daar wordt de data gebruikt voor transformaties en analyses.

Verdere verwerking parallel aan het proces:

Behandelen Bezwaar en beroep

Het behandelen van bezwaar en beroep, vastleggen van de uitkomst en bij toegekend bezwaar mogelijkheid tot aanmaken beschikking besluit op bezwaar. Als er van een deskundige iets nodig is in het bezwaarproces, wordt Atabix gebruikt. Dit gebeurt bij een nader advies of het inplannen van een hoorzitting.

Herstel in Natura (HIN)

HIN is gerealiseerd door Atabix als een onafhankelijke applicatie, niet geïntegreerd met de basis Atabix applicatie. Ook HIN is gerealiseerd als een zaaksysteem, met een beperkt aantal stappen. Als een aanvrager kiest voor herstel in natura in plaats van een vergoeding wordt een dossier na akkoord op de beoordeling overgedragen naar de applicatie HIN.

Het HIN proces is eenvoudig qua applicatieve ondersteuning:

De HIN medewerker importeert een HIN-dossier uit de basis Atabix applicatie. Hij plant de herstelactie in en wijst ze toe aan één van de drie herstelbedrijven. Het herstelbedrijf toetst en accepteert de opdracht en voert het herstel uit. Als wordt geconstateerd dat het herstel meer omvat dan de oorspronkelijke opdracht kan de opdracht worden bijgesteld. De aannemer kan individuele schades afvangen als "herstel gereed". Dat doet niet elke aannemer.

Na gereed melding wordt op basis van de schades een opnameformulier cq prestatieverklaring gegenereerd. Die wordt vervolgens op locatie met de aanvrager getekend door alle partijen.

Algemene applicatiefuncties:

- identificatie, authenticatie en autorisatie
- communicatiemomenten registreren
- workflow (Voorbereiding, Wachten op ondertekening, Opdracht aangenomen, Werkzaamheden gestart, ..)
- dashboards rapportage en prognose

Uitgangspunt: HIN kent **geen integratie met de basis Atabix applicatie**.

Er is alleen een import van dossiers vanuit Atabix naar HIN. Daarna vindt de afhandeling volledig in HIN plaats.

NB: in de huidige implementatie is er wel een gedeeld gebruik van onder meer persoonsgegevens met de basis Atabix applicatie, maar die is niet gewenst.

• \

Verwerking 5: Datamigratie Atabix 1.3

De datamigratie is een uitvloeisel van programma Uniformeren. Het wordt als een klein project gezien, met als aanspreekpunt **5.1.2e** (adviseur Informatievoorziening – afdeling Regiebureau).

Het idee is om eerst te kijken naar een migratie van 140.000 dossiers met een bepaalde status van 1.3 naar 2.0. Ongeveer 95% van deze dossiers hebben de status afgewikkeld en/of afgebroken.

Verder wil men de dossiers in 'Bezwaar en Beroep' gaan migreren van 1.3 naar 2.0.

Planning (voor nu):

- 3^e week van april PvA klaar
- Mei - testen met migratie -
- Juni (en 3 maanden daarna) bezig met migreren

5.1.2e en **5.1.2e** van Valcon zijn bezig met de opmaak van een plan van aanpak, planning en budget.

Testen met gegevens

Men was voornemens om een eigen testomgeving te gaan gebruiken, maar aangezien Atabix (leverancier) zelf een OTAP omgeving heeft, wil het IMG gebruik gaan maken van deze omgeving van Atabix. Dit betreft een verdere verwerking van persoonsgegevens in de zin van artikel 6 lid 4 AVG. Hiervoor dient eigenlijk een toets te worden gehouden, anders mag de test niet plaatsvinden. Dit lijkt op dit moment een verdompen feit. Daarnaast dienen betrokkenen hier eigenlijk over te worden geïnformeerd.

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van

persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Bij Atabix worden persoonsgegevens voor de volgende doeleinden verwerkt:

- Het behandelen van de schade aanvragen conform de Tijdelijke wet Groningen;
- Het behandelen van Herstel in Natura (HIN) aanvragen;
- Beschikkingen (besluiten) waarbij een toekenning van de vergoeding is bepaald, een correcte financiële afwikkeling (uitbetaling) te waarborgen;
- Indien de aanvrager een bezwaarschrift indient tegen de beschikking (besluit), dient het IMG een correcte afwikkeling van het bezwaar en daarbij behorende besluit te garanderen.

Met het gebruik van Atabix wordt door het IMG invulling gegeven aan de aan hem opgedragen wettelijke plicht uit de Tijdelijke wet Groningen.

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de

verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Bij deze verwerking zijn de volgende partijen betrokken:

Verwerkingsverantwoordelijke:

- De minister van EZK, namens deze de voorzitter TCMG
- De projectdirectie TCMG van de RVO.nl, voor het beschikbaarstellen van mensen en middelen aan de voorzitter TCMG

Verwerker

- Atabix Solutions B.V.
- Externe bureaus die de schade opnemen
- Amazon Web Services Europe (Amazon Web Services EMEA SARL)

Toegang tot de gegevens

Ontvangers van persoonsgegevens:

- Behandelend medewerkers van de opdrachtgever
- Behandelend medewerkers van de wederpartij
- Behandelend medewerkers van door de wederpartij gecontracteerde subverwerkers
- Auditdienst Rijk
- Degenen die binnen TCMG belast zijn met de werkzaamheden ten behoeve van de beschreven doelen van deze verwerking

- DICTU (Dienst ICT Uitvoering)

Verstrekken van persoonsgegevens

- Woningcorporaties
- Particuliere verhuurders van woningen en bedrijfspanden
- Aanvrager (bewoner en intermediair)
- Deskundigen
- Logius (DigiD)
- Relatieservices RVO – Basisregistratie Personen (BRP) via MIRA
- Kadaster
- Gebruikers
- NAM

Ontvangers van persoonsgegevens

- Auditdienst Rijk
- DICTU
- Behandelend medewerkers IMG
- Gebruikers Atabix
- KPMG
- ADC (Amsterdam Data Collective) – data analyse
- ABT – data analyse
- Het herstelbedrijf – aannemers (m.b.t. HIN)

Gebruikers Atabix (intern)

- Regiebureau (inzage in Atabix)
 - Ontwikkeling en Beheer
 - Productie, Advies en Gegevens
- Klantcontact en -dienstverlening
 - Planning
 - Werkvoorbereiding
 - Zaakbegeleiding
- Schade expertise en herstel
 - Acut Onveilige Situatie
 - Herstel in Natura
 - Toetsing
 - Prestatiesturing (sturend richting de partijen)
- Bestuurlijke en Juridische Zaken en Schadeafhandeling
 - Fysieke Schade Regulier
 - Fysieke Schade Complex
 - Waardedaling en Immaterieel
 - Bestuurlijk en Juridisch Advies
 - Bezwaar en Beroep (inzage in Atabix)

Functionarissen (zie autorisatiematrix Atabix)

- Service Loket medewerker
- Zaakbegeleider
- Planning
- Werkvoorbereiding
- Functioneel beheer IMG
- Interne control/ auditor IMG
- Financieel team (betaalproces)
-

6. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Het belang van de verwerkingsverantwoordelijke inzake de verwerking van persoonsgegevens is om een besluit te kunnen nemen op de aanvraag en indien van toepassing de financiële afwikkeling van de mijnbouwschade.

Daarnaast is het belang van de gegevensverwerking(en).

- Locatiebepaling a.d.h.v. adresgegevens.
- Content van het adviesrapport (o.b.v. persoonsgegevens)
- Afspraken maken voor schadeopname/hoorzitting (NAW-gegevens, telefoonnummer etc.)
- Dossieroverzicht in Atabix

Belang van de aanvrager of intermediair voor een snelle afwikkeling en het spoedig vergoed krijgen van (eventuele) mijnbouwschade aan eigendommen, zodat leefbaarheid gegarandeerd blijft.

Tot slot is het belang van Atabix dat zij het IMG goed ondersteunen bij de uitvoering van de primaire taak.

7. Verwerkingslocaties



Benoem in welke landen de voorgenoemde gegevensverwerkingen plaatsvinden.

De verwerkingsverantwoordelijke (IMG) is in Groningen (Nederland) gevestigd.

Verwerker(s):

- Atabix is gevestigd in Amsterdam en verwerkt gegevens mogelijk in Duitsland (staan de servers) (en de Verenigde Staten (via AWS)).
- DICTU is gevestigd in Nederland en verwerkt uitsluitend in Nederland.
- Deskundigenpartijen zijn in Nederland gevestigd en verwerken persoonsgegevens uitsluitend in Atabix.

En (eventuele) belanghebbenden:

- Auditdienst Rijk is gevestigd in Nederland en verwerkt gegevens in Nederland.
- RVO is gevestigd in Nederland en verwerkt gegevens in Nederland.

8. Techniek en methode van gegevensverwerking



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

[Klik hier om infotekst te verbergen](#)

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

- a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
- c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

- a. wettelijk is toegestaan; en
- b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

Alle data die zich op enig moment in Atabix bevindt wordt middels AES256 encryptie in de database opgeslagen. Toegang tot Atabix wordt beveiligd met zogenaamde tweefactorauthenticatie (gerealiseerd eerste week juli 2019).

De data wordt vanuit de TCMG handmatig via het SSL encryptieprotocol (versie TLS 1.2) beveiligde verbinding in de applicatie geplaatst wanneer er vanuit een schade-expert hier een verzoek voor komt. De in Atabix aanwezige (versleutelde) data blijft voor een beperkte periode beschikbaar. Op het moment dat de schade expert de schadeopname heeft afgerond en het rapport door TCMG is geaccepteerd, wordt de data in de applicatie Atabix verwijderd.

Na verwijdering blijft de data nog 35 dagen in de back-up aanwezig.

9. Juridisch en beleidsmatig kader



Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

De Tijdelijke wet Groningen bevat regels over het IMG als organisatie, inclusief zijn taken en bevoegdheden. Met de TwG (per 1 juli 2020) is de afhandeling van alle schade als gevolg van bodembeweging door aanleg of exploitatie van een mijnbouwwerk ten behoeve van gaswinning uit het Groningenveld of gasopslag bij Norg door de overheid wettelijk geregeld.

Voor het verwerken van het BSN geldt specifieke regelgeving, zie daarvoor het antwoord onder 12. Voor deze DPIA is BSN niet relevant, aangezien BSN niet in Atabix voorkomt.

Tevens is onder andere de volgende wetgeving van toepassing:

- Archiefwet
- Algemene Wet Bestuursrecht
- Wet open overheid (Woo)
- Wet basisregistratie personen
- Wet algemene bepalingen Burgerservicenummer
- Informatiebeveiligings- en privacybeleid IMG

Tot slot heeft de Baseline Informatiebeveiliging Overheid (BIO) gevolgen voor de gegevensverwerkingen binnen Atabix (zie QuickScan IB - RVO-I2106 4200). Advies deze Quickscan te updaten.

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij **conceptregelgeving** zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij **overheidsverwerkingen** moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.

Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegevens	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

In de generieke Selectielijst wordt onder andere besproken de zogenaamde "Kritische Onderwerpen" of ook wel genoemd "HotSpots". HotSpots zijn gebeurtenissen of ontwikkelingen die een grote impact hebben op de relatie tussen de overheid en burgers of op burgers onderling. De archieven van het IMG, inclusief rechtsvoorgangers en rechtsopvolgers zijn voorlopig aangewezen als 'hotspot'. Dit houdt in dat alle archieven van het IMG lange tijd bewaard moeten worden. In de maatregelen is opgenomen dat de bewaartermijnen worden herzien.

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

De persoonsgegevens zijn te bewaren indien ook de zaakdossiers waarin de schadeclaims worden

behandeld tot de 'hotspot' worden gerekend. Indien in een later stadium anders wordt bepaald kunnen de persoonsgegevens in principe worden vernietigd als het pand waarop de schadeclaims rusten in andere handen over gaat. Voor dit moment is dat nog niet aan de orde.

Er gaan momenteel geen stukken naar het Nationaal Archief. Wanneer bepaalde stukken worden gecategoriseerd met een B (van bewaren), dan moeten deze stukken voor altijd worden bewaard. Alles met een B wordt na 20 jaar overgebracht worden naar het Nationaal Archief (volgens de Archiefwet).

Het advies van DIV-RVO moet worden heroverwogen om duidelijkheid te krijgen of er daadwerkelijk sprake is van een 'hotspot' en of persoonsgegevens blijvend moeten worden bewaard. Daarnaast is het de vraag, als de persoonsgegevens gearhiveerd zijn, of deze nog bewaard moeten worden in Atabix. Daarvoor moet een bewaartermijn worden opgesteld.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

[Klik hier om infotekst te verbergen](#)

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

- a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de

verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

Atabix wordt ingezet voor het uitvoeren van de wettelijke taak (art. 6 lid 1 sub c) van het IMG, namelijk het afhandelen van schade veroorzaakt door gaswinning uit het Groningenveld en de gasopslag Norg. De rechtsgrond voor de gegevensverwerking door IMG ligt in ex art. 2 jo. art. 3 van de Tijdelijke wet Groningen, waarin expliciet wordt gemaakt dat ten behoeve van de taken van het instituut en de exploitant persoonsgegevens worden verwerkt. Er is daarom een wettelijke verplichting om persoonsgegevens te verwerken.

De grondslag van art. 6 lid 1 sub c AVG bevat het vereiste 'noodzakelijkheid', wat kort gezegd inhoudt dat de verwerking noodzakelijk is om aan de wettelijke plicht te kunnen voldoen. Atabix wordt daarbij ingezet om schades beter te kunnen vastleggen, communicatie met de aanvrager te verbeteren en de afhandeling van het schadeproces verder te uniformeren.

Het IMG kan zonder het gebruik van Atabix niet haar wettelijke taak uitvoeren. Er is geen andere manier/ applicatie om schades mee op te nemen.

Doordat Atabix de enige partij is die de schadeopname applicatie heeft ontwikkeld en beheert, is het dan ook nodig dat zij gegevens verwerken om de verwerkingsdoeleinden te realiseren.

- De persoonsgegevens worden verwerkt in Atabix ten behoeve van de volgende regelingen:
- Fysieke schade – schade aan gebouwen en objecten – Regulier proces
 - Herstel in Natura (aparte omgeving in Atabix) → vallend onder Schade Expertise & Herstel (SEH)
 - VES – vaste vergoeding voor schade aan woningen – Atabix alleen voor de planningstool
 - Immateriële schade - Atabix alleen voor de planningstool
 - Ambtelijk bezwaar
 - Bezwaar

Het verwerken van deze persoonsgegevens in de applicatie Atabix moet noodzakelijk zijn voor het kunnen beoordelen van aanvragen. Een risico daarbij is dat nog niet helder is welke persoonsgegevens ten behoeve van welke regelingen worden verwerkt. Bovendien is niet duidelijk van welke soort betrokkene (aanvrager, intermediair, deskundige of gebruiker) de verwerkte persoonsgegevens zijn. Daardoor kan niet goed beoordeeld worden of de verwerking noodzakelijk is voor het uitvoeren van de wettelijke verplichting en daarmee of aan de eisen van proportionaliteit is voldaan.

12. Bijzondere persoonsgegevens



Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

[Klik hier om infotekst te verbergen](#)

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

- de betrokkene heeft uitdrukkelijke toestemming gegeven;
- de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
- de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
- de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
- de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor

doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

- a. wettelijk is toegestaan;
- b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
- c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij **conceptregelgeving** kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

In Atabix behoren geen bijzondere (en gevoelige) persoonsgegevens te worden verwerkt. Wel is er een risico op bijvangst door het nemen van foto's of iets dergelijks. Uit foto's van werk, woon- en verblijfsruimten, inclusief persoonlijke eigendommen kunnen persoonlijke voorkeuren blijken. Hierdoor bestaat het risico dat er bijzondere- en/of gevoelige persoonsgegevens worden verwerkt. Hiervoor dienen waarborgen te komen, zodat er geen bijzondere/gevoelige persoonsgegevens in rapporten komen.

Een ander risico is dat voor de regeling omtrent immateriële schadevergoeding de planningstool in Atabix wordt gebruikt. Uit de DPIA IMK blijkt dat er geen hoorzittingen worden gepland voor de regeling IMS dan wel IMK. Daarbij moet voorkomen worden dat de ingevulde vragenlijst over de persoonlijke impactanalyse en bewijsstukken in Atabix worden verwerkt, omdat deze gegevens over de gezondheid kunnen bevatten

13. Doelbinding



Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, oordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

- het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
- de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

- de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

De verzamelde persoonsgegevens worden alleen voor de doeleinden (onder paragraaf 4) gebruikt. Het IMG (verwerkingsverantwoordelijke) verwerkt daarbij gewone persoonsgegevens met als doel om het afhandelen van schade veroorzaakt door gaswinning uit het Groningenveld en de gasopslag Norg (ex art. 2 jo. art. 3 van de Tijdelijke wet Groningen). Persoonsgegevens mogen alleen voor die doeleinden of daarmee verenigbare doelen verder worden verwerkt. Dat is het geval bij de verwerking in Atabix. De verwerking van persoonsgegevens is nodig voor het opmaken van een adviesrapport om uiteindelijk tot een beoordeling van de aanspraak op schadevergoeding te komen. Indien verwerking voor een ander doel dan de genoemde doelen noodzakelijk is zal door het Instituut aan de hand van de AVG moeten worden gezien of hier een grondslag voor is en of de verwerking hiervoor noodzakelijk is.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- a. Proportionaliteit:** staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- b. Subsidiariteit:** kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.

De gegevensverwerking vindt plaats met inachtneming van de doelen in paragraaf 4. De verwerking van de persoonsgegevens moet in verhouding staan tot het doel van het behandelen van de aanvragen tot schadevergoeding. De verwerking van IP-adressen is nodig om informatie van DigiD naar Atabix te transporteren. Het BSN-nummer, de NAW-gegevens en geboortedatum zijn noodzakelijk om een aanvrager of intermediair te identificeren. Bovendien is het telefoonnummer en e-mailadres nodig om contact op te nemen over de aanvraag. Deze persoonsgegevens zijn daarmee nodig voor het behandelen van aanvragen conform de Tijdelijke wet Groningen, het behandelen van HIN aanvragen, het toekennen van een beschikking en het behandelen van bezwaren. Daarom staat de inbreuk op de persoonlijke levenssfeer in verhouding tot de verwerkingsdoelen (proportionaliteit)

De verwerkingsdoelen kunnen niet op een andere manier bereikt worden, omdat geen andere persoonsgegevens verwerkt kunnen worden die de aanvrager met voldoende zekerheid kunnen identificeren en waardoor er contact met de aanvrager opgenomen kan worden. In paragraaf 11 is ook vastgesteld dat de Atabix applicatie noodzakelijk is voor de doelstellingen. Hiermee is ook voldaan aan het vereiste van subsidiariteit.

Het is echter niet proportioneel om de persoonsgegevens langer te bewaren van noodzakelijk is voor de doelstellingen. Het volgende is onduidelijk over de bewaartermijnen:

- De periode waarin gegevens in Atabix worden bewaard nadat het adviesrapport is opgeleverd is onduidelijk, want er zijn geen bewaartermijnen. Het gaat om de opnametool, trillingstool en peTAT. Dit geldt ook voor documenten die worden geüpload in het kader van bezwaar en beroep.
- Het is niet helder of de persoonsgegevens bewaard moeten blijven voor archivering (paragraaf 10).

Bovendien is het niet proportioneel om meer persoonsgegevens te verzamelen dan noodzakelijk voor het doel. Daarom mogen via de koppeling met MIRA geen andere persoonsgegevens toegankelijk zijn dan opgesomd in paragraaf 2. Bovendien mogen deskundigen in Atabix niet meer persoonsgegevens inzien dan noodzakelijk voor het opstellen van een adviesrapport voor een bepaalde regeling. Er is geen duidelijke definitie van de rollen en verantwoordelijkheden vastgesteld en de proceseigenaar voor Atabix is onduidelijk. Verder wordt metadata bij foto's verzameld: dat is niet nodig voor het bereiken van de doelstellingen.

Ook worden persoonsgegevens gedeeld met een aantal ontvangers. Deze mogen niet meer persoonsgegevens verwerken dan noodzakelijk voor het behalen van de doelstellingen. Er moet daarom vastgesteld worden of, en welke persoonsgegevens de herstelbedrijven ontvangen in het kader van HIN, waar deze persoonsgegevens worden opgeslagen en gedurende welke periode. Voor andere verwerkers is een (concept) verwerkersovereenkomst opgesteld of gaat deze

opgesteld worden. Tot slot is de subverwerker van Atabix AWS, maar niet uitgesloten kan worden dat persoonsgegevens ook in de Verenigde Staten worden verwerkt.

15. Rechten van de betrokkene



Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

De AVG geeft aan de betrokkenen van de gegevensverwerking een aantal rechten die zij jegens de verwerkingsverantwoordelijke kunnen uitoefenen. Deze staan genoemd in artikel 15-21 van de AVG. In de privacyverklaring van IMG is meer informatie te vinden over hoe een betrokkene een beroep kan doen op een of meer van deze rechten.

Intern bestaat een handleiding rechten van betrokkenen waarin staat uitgewerkt welke handelingen worden verricht bij een verzoek met betrekking tot de rechten van betrokkenen. Het is onvoldoende duidelijk welke procedures er zijn ingericht tussen IMG en Atabix en tussen Atabix en Amazon Web Services Europe over de behandeling van AVG-verzoeken.

De privacyverklaring is terug te vinden op de website van het IMG. Tevens wordt deze verklaring aangeboden bij het indienen van een aanvraag.

Ook kunnen zaakbegeleiders informeren over privacy-rechten, omdat zij regelmatig contact hebben met de betrokkenen.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- de oorsprong van deze gevolgen;**
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

[Klik hier om infotekst te verbergen](#)

Volgens de privacyregulering dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de

gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- waar de gegevensverwerking kan leiden tot:
 - discriminatie, stigmatisering en uitsluiting;
 - (blootstelling aan) identiteitsdiefstal of -fraude;
 - financiële verliezen;
 - reputatie- of anderszins relationele schade;
 - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
 - ongeoorloofde ongedaanmaking van pseudonimisering;
 - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
 - wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
 - wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
 - wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;

- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens. Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
 - wijziging (integriteit);
 - ongeoorloofde toegang en verstrekking (vertrouwelijkheid);
- van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.

Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

Beveiliging van de verwerking

- Op dit moment is er onvoldoende duidelijkheid over de door Atabix Solutions BV getroffen en met Amazon Webservices Europe afgesproken maatregelen. Zie voor verdere uitleg hiervoor de Quickscan BIO Quickscan BIO - Atabix - D1.0 - RVO-I1904 1989 en Bijlage Quickscan BIO - Atabix - Openstaande vragen D1.0 - RVO-I1904 1989

Gevolgen Cloud act

- Als Amerikaans bedrijf is de Amerikaanse Cloud Act van toepassing op Amazon. Niet uitgesloten kan worden dat er gegevens gevorderd worden door Amerikaanse veiligheidsdiensten.

Rechten van de betrokkene

- Het is onvoldoende duidelijk welke procedures er zijn ingericht tussen TCMG en Atabix en tussen Atabix en Amazon Webservices Europe over de behandeling van AVG-verzoeken.

Bijzondere persoonsgegevens

- Tijdens de schadeopnamen worden foto's gemaakt van de binnen- en buitenzijde van het object. Uit foto's van werk, woon- en verblijfsruimten, inclusief persoonlijke eigendommen kunnen persoonlijke voorkeuren blijken.

Datalekprocedure

- Het is onvoldoende duidelijk welke procedures er zijn ingericht tussen Atabix en Amazon Webservices Europe over het melden van datalekken.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen



Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

[Klik hier om infotekst te verbergen](#)

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op

een dusdanige manier wordt 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.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht. Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

- a. pseudonimiseren en versleutelen van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;

- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

- a. controle op de toegang tot de apparatuur;
- b. controle op de gegevensdragers;
- c. opslagcontrole;
- d. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelmogelijkheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van

de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Beveiliging van de verwerking

- Als vervolg op de Quickscan BIO moeten de openstaande vragen via de gap-analyse worden beantwoord.

Gevolgen Cloud act

- De bij Amazon Webservices Europe opgeslagen gegevens zijn versleuteld met de AES256 technologie. Dus alle data in het systeem is AES256 encrypted. Gebruikerswachtwoorden en sleutels zijn bovendien met een salt encryptie opgeslagen en zijn daardoor niet te decoderen.

Rechten van de betrokkene

- Met Atabix Solutions BV moeten afspraken worden gemaakt over afhandeling van AVG-verzoeken. Deze zijn ook van toepassing op Amazon Webservices BV.

Bijzondere persoonsgegevens

- Foto's waar mogelijk kenmerken van ras of etnische afkomst of religieuze of levensbeschouwelijke overtuigingen (bijv. voorwerpen) van zijn af te leiden, dienen goed geblurd te worden. Door te blurren (maatregel) zijn deze persoonsgegevens voldoende afgeschermd.
- De voornoemde foto's dienen tot aan het moment dat deze geblurd worden, op passende wijze beveiligd te worden. Bijvoorbeeld via encryptie.
- De originele, niet geblurde, foto's moeten direct nadien vernietigd worden.

Datalekprocedure

- Met Atabix Solutions BV moeten afspraken worden gemaakt over de melding van datalekken. Deze zijn ook van toepassing op Amazon Webservices BV.

In 2023 zijn dit de maatregelen die inmiddels reeds zijn genomen bij Atabix (privacy/security) in vergelijking met 2018:

- Afscheiden van noodzakelijke gegevens vanuit Mira die nodig zijn voor de processen en het opstellen van het adviesrapport. Hierdoor worden alleen de gegevens uit Mira gehaald die nodig zijn voor het proces en het opstellen van het adviesrapport.
- MFA/2FA (Multi Factor Authentication) bij inloggen gebruikers. Daarmee wordt voldaan aan IAM eisen.
- Rolomschrijving, dus wat je nodig hebt voor een bepaalde rol en alleen dat uitvoeren door middel van werkinstructies.
- Tooling die beschikbaar komt voor bepaalde afdelingen, wordt alleen beschikbaar gesteld voor afdelingen die de tooling nodig hebben.
- Atabix is ISO/IEC 27001 gecertificeerd als organisatie.

Bijlage 1 – Risico register - Risico's en maatregelen

Risico register

	Risico	Gevolgen	Maatregel	Actiehouder	Status	Einddatum
1	De toegang tot persoonsgegevens moet passend beveiligd zijn. Een risico is dat met het toekennen van een bepaald autorisatieprofiel toegang verkregen kan worden door onbevoegden. Er is een risico op identiteitsdiefstal en verlies van vertrouwelijkheid.	Hierdoor is de kans dat onbevoegden toegang hebben tot persoonsgegevens van aanvragers en mogelijk hier misbruik van maken. Er wordt reeds gebruik gemaakt van meerfactorauthenticatie (MFA).	Er kan bijvoorbeeld gewerkt worden met een beleid met voorwaardelijke toegang voor herkende gebruikers, zodat zij niet altijd meerfactorauthenticatie hoeven te gebruiken.	Proces-eigenaar	Nog uit te voeren	Nader te bepalen
2	Bij de schadeopname wordt beeldmaterieel gemaakt van de binnen- en buitenzijde van het object. Uit foto's van werk, woon- en verblijfsruimten, inclusief persoonlijke eigendommen kunnen persoonlijke voorkeuren blijken. Hierdoor kunnen er bijzondere- en/of gevoelige persoonsgegevens worden verwerkt (vastgelegd).	Doordat het verwerken van bijzondere en/of gevoelige persoonsgegevens in Atabix niet noodzakelijk is, is de kans aanwezig dat onbedoeld deze persoonsgegevens worden verwerkt (eventuele bijvangst).	Opstellen van werkinstructie waarin de bijvangst aan bijzondere en/of gevoelige persoonsgegevens wordt voorkomen.	Proces-eigenaar	Uitgevoerd	n.v.t.
3	Persoonsgegevens worden (onrechtmatig) langer bewaard in Atabix (cloud) dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze is verzameld.	Het is niet duidelijk hoe lang de gegevens in Atabix worden bewaard en of nadat het rapport is opgeleverd de gegevens worden verwijderd/vernietigd.	Het IMG heeft geen gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens in Atabix. Er dient een gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens worden opgesteld. Er moet bovendien	Proces-eigenaar	Nog uit te voeren	Nader te bepalen

			gecontroleerd worden of het beleid wordt nageleefd, nadat deze is opgesteld en geïmplementeerd.			
	De persoonsgegevens moeten langer bewaard blijven dan noodzakelijk zolang onduidelijk is of de persoonsgegevens gearhiveerd moeten worden.	De persoonsgegevens kunnen niet verwijderd worden en als dat wel gebeurt, kan achteraf blijken dat deze toch bewaard hadden moeten blijven omdat er een 'hotspot' is.	Het advies van DIV-RVO moet worden heroverwogen om duidelijkheid te krijgen of er daadwerkelijk sprake is van een 'hotspot' en of persoonsgegevens blijvend moeten worden bewaard.	Proces-eigenaar	Nog uit te voeren	Nader te bepalen
4	Uit gesprekken met Juridische Zaken blijkt dat met name vanuit de bezwaarprocedures zeer veel documenten in Atabix worden geüpload, welke van belang zijn voor de deskundigen in het beoordelen en informeren ten behoeven van hoorzittingen, e.d. Na afronding van de bezwaarprocedure blijven deze documenten op Atabix bewaard , zonder enig aanleiding en doel om deze daar te bewaren.	Doordat na afronding van de bezwaarzaak de documenten niet uit Atabix worden verwijderd, is de kans op beveiligingsincidenten groot.	Het IMG heeft geen gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens in Atabix. Er dient een gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens worden opgesteld. Duidelijke afspraken maken over het verwijderen van documenten in Atabix na afsluiten dossier.	Proces-eigenaar	Nog uit te voeren	Nader te bepalen
5	Het gebruik van metadata bij foto's.	Gevolgen grootschalige verwerking van metadata (DPIA-plichtig en dus hoog risico volgens de AP). Hierbij dient dataminimalisatie worden getracht.	Verwijder metadata bij het uploaden van de foto of stel een protocol op voor het gebruik/beveiligen ervan, zodat er passende technische en organisatorische maatregelen zijn.	Proces-eigenaar	Nog uit te voeren	Nader te bepalen
6	Het gebruik AWS (externe cloudoplossing) door Atabix, waar gegevens van aanvragers worden opgeslagen. Hierdoor worden mogelijk persoonsgegevens buiten de Europese	Als Amerikaans bedrijf is de Amerikaanse Cloud Act van toepassing op Amazon. Niet uitgesloten kan worden dat er gegevens gevorderd	Vanuit Atabix meer duidelijkheid krijgen hoe de gegevens op AWS worden opgeslagen en verder worden verwerkt. Daarnaast kan encryptie worden gebruikt op servers in de	Proces-eigenaar	Nog uit te voeren	Nader te bepalen