

Inleiding

Voeg hier wanneer gewenst een openingsalinea of inleiding toe. Denk bijvoorbeeld aan:

- Verwijzing naar het privacybeleid of motivatie achter de uitvoering van deze PIA
- Informatie over de manier van opstellen.

Vanaf 1 november 2021 heeft de bewoner (nieuwe aanvrager) bij het Instituut Mijnbouwschade Groningen (hierna: het IMG) de mogelijkheid te kiezen voor een vaste vergoeding (hierna: VES regeling).

Voorwaarde om mee te doen aan de VES regeling is dat de aanvrager nog niet eerder een aanvraag tot schadevergoeding heeft ingediend bij het Instituut, de TCMG, CVW of de NAM. Uitgezonderd zijn objecten¹ waarvoor reeds eerder een melding is gedaan bij NAM/CVW en/of TCMG/IMG, tenzij op die melding bij TCMG/IMG nog geen besluit op de aanvraag is genomen.

Daarnaast geldt dat de vergoeding als finaal geldt, tenzij zich een nieuwe aardbeving voordoet die op locatie een trilling van minimaal 5 mm/s veroorzaakt.

De VES is een onderdeel van de regeling voor fysieke schade en werken². Maar wat houdt de vaste vergoeding in?

- Een eenmalige vergoeding voor een eerste schademelding voor een object.
- Een vast bedrag dat alle schade aan het object vergoedt en afhandelt.
- Bedoeld voor de afhandeling van kleine, niet ingewikkelde schades.
- Eenvoudige en automatische aanvraag, snelle doorlooptijd en uitkering.
- Geen deskundige over de vloer, geen adviesrapport nodig.
- Bewijsmateriaal: eigen foto's of een nulmeting.

De VES regeling is een beleidsregel en geen ministeriële regeling of AMvB doordat de regeling door het IMG zelf wordt vastgesteld als zelfstandig bestuursorgaan. Doordat er binnen de VES regeling, welke een invulling is aan de wettelijke taak van het IMG ex art. 2 jo. art. 3 van de TwG, gebruik wordt van vele persoonsgegevens, vermoedelijk 200.000 aanvragen (**grootschalige verwerking**), gecombineerd met **geautomatiseerde besluitvorming** en **eventuele grootschalige communicatiegegevens (metadata)**, is een **DPIA** noodzakelijk.

De resultaten van deze DPIA worden gebruikt om de organisatie meer bewust te maken van het belang om aan privacybescherming te doen en maatregelen door te voeren om de privacy van de aanvragers (betrokkenen) beter te beschermen/borgen.

¹ Een object is een onroerende zaak met een eigen kadastrale aanduiding met daarop ten minste één adres. U kunt een vaste vergoeding alleen aanvragen voor een volledig object. Daarbij gaat het meestal om een woning. Maar het kan ook om een woning én een schuur gaan. Of om een appartement of een winkelpand. Ook kan het gaan om een pand met meer dan één huisnummer.

² Meer informatie hierover is te vinden op de website van IMG onder [Schade aan gebouwen en objecten](#).

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Per 1 november 2021 lanceert het IMG de VES-regeling, een regeling waarbij aanvragers aanspraak kunnen maken op een éénmalige vaste vergoeding van € 5.000,- voor hun schade.

Voorwaarde om mee te doen aan de regeling is dat de aanvrager nog niet eerder een aanvraag tot schadevergoeding heeft ingediend bij het Instituut, de TCMG, CVW of de NAM. Uitgezonderd zijn objecten waarvoor reeds eerder een melding is gedaan bij NAM/CVW en/of TCMG/IMG, tenzij op dat melding bij TCMG/IMG nog geen besluit op de aanvraag is genomen.

Daarnaast geldt dat de vergoeding als finaal geldt, tenzij zich een nieuwe aardbeving voordoet die op locatie een trilling van minimaal 5 mm/s veroorzaakt.

Voor de VES-regeling geldt een andere werkwijze dan bij fysieke schade. Er wordt geen gebruik gemaakt van een deskundige die een opname verricht. In plaats daarvan draagt de aanvrager zelf zorg voor het verstrekken van foto's van de schade, of er wordt een nulmeting verricht. In het laatste geval worden de schades niet beoordeeld, maar legt de deskundige de schade uitsluitend in een rapportage vast met foto's.

De VES-regeling sluit voor het grootste deel aan bij het reguliere proces dat het IMG heeft ingericht voor het vergoeden van fysieke schade. Redenen om toch een aparte DPIA uit te voeren bij de VES-regeling zijn dat de VES-regeling in potentie een zeer groot bereik kent van 100.000-200.000 aanvragers die hier in potentie aanspraak op zouden kunnen maken, in combinatie met het feit dat er mogelijk gebruik wordt gemaakt van beeldherkenning en automatische besluitvorming. Daarnaast betekent het feit dat aanvragers zelf foto's van schades gaan uploaden naar een omgeving van het IMG, dat er sprake is van verwerking van een grootschalige hoeveelheid data en metadata, en dit brengt potentiële risico's met zich mee.

2. Persoonsgegevens

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 persoonsgegevens. 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 overgeërfd 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 marketingdoeleinden, 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.

Bij de VES-regeling worden verschillende categorieën persoonsgegevens verwerkt, die voor het grootste deel overeen stemmen met de categorieën persoonsgegevens die in het kader van de reguliere procedure voor vergoeding van fysieke schade worden verwerkt.

Gewone persoonsgegevens:

- Naam, geslacht, adres, woonplaats gegevens van aanvragers;
- Contactgegevens zoals telefoonnummer en/of e-mailadres;
- Bankrekeningnummer (IBAN);
- Foto's van schadeplek; op deze afbeeldingen kan nadere informatie zichtbaar zijn,

- waaronder (bijzondere) persoonsgegevens;
- IP-adressen (niet vastgelegd of bewaard);
- Eigendoms- en pandgegevens zoals bekend bij het Kadaster.

Bijzondere persoonsgegevens:

- In principe worden geen bijzondere persoonsgegevens verwerkt, maar deze kunnen zich eventueel bevinden in het beeldmateriaal dat aanvragers zelf indienen bij het IMG.

Wettelijk identificerende persoonsgegevens:

- Het IMG verwerkt het Burgerservicenummer (BSN) van zijn aanvragers.

3. Gegevensverwerkingen

i

Geef alle voorgenumen gegevensverwerkingen weer.

In deze paragraaf worden de voorgenumen gegevensverwerkingen binnen de VES-regeling toegelicht.

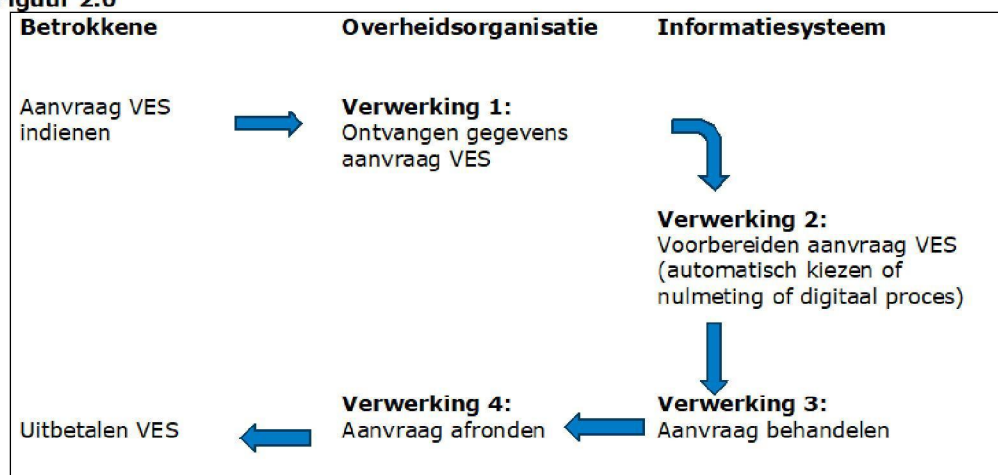
De VES procedure wordt in figuur 2.0 visueel (workflow) weergegeven. Het figuur geeft ook inzicht in het geheel van bewerkingen betreffende persoonsgegevens (gegevensverwerking) zoals bedoeld in art. 4 lid 2 van de AVG. Een gegevensverwerking is het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

De processtappen worden aan de hand van een toelichting van het projectteam per stap toegelicht. Daarnaast is gekeken naar de procesbeschrijvingen van deze regeling, welk in concept zijn opgesteld door procesbeheer.

De procesbeschrijvingen zijn niet volledig beschreven dan wel vastgesteld door de proceseigenaar met de mogelijke risico's van dien.

- VES Indienen en Registreren, Voorbereiden, Plannen en Schade opnemen (fase 2a en 3)
- VES Voorbereiden besluit en Beoordelen besluit (fase 2a en 3)

Figuur 2.0



Verwerking 1: Aanvragen en ontvangen van de aanvraag (indienen en registreren aanvraag) (KCDV)

De VES-regeling begint altijd met het doen van een aanvraag. Gelet op het geautomatiseerde karakter van het proces, geniet het de voorkeur om dit door middel van DigiD te doen. Eigenaar (aanvrager) meldt zijn/haar schade in 'Mijn dossier'. Daarvoor dient men in te loggen via DigiD. De eventuele mede-eigenaar dient ook akkoord te zijn met de aanvraag. Daarvoor moet hij/zij toestemming geven in hun eigen 'Mijn dossier' door eveneens in te loggen met DigiD.

De aanvrager wordt via DigiD geïdentificeerd/geauthentiseerd op basis van een aantal controle gegevens (bijvoorbeeld BSN en geboortedatum). Na het inloggen via DigiD kan aanvrager een schade aanvraag indienen via het IMG portaal (Mijn dossier). Daarbij worden de eigendommen van de aanvrager uit het Kadaster opgehaald.

Aanvragers die wonen op een VES geschikte adres krijgen naast de reguliere schade afhandeling (c.q. maatwerk) ook de optie van 'Vaste Vergoeding' aangeboden.

Wanneer deze optie wordt aangevinkt wordt op basis van de trillingssterkte en het bouwjaar van het object (schadeadres) bepaald of er een nulmeting moet komen.

Om voor de vaste vergoeding in aanmerking te komen heeft het IMG een keuzehulp op de website, waarbij aan de hand van postcode en huisnummer en bouwjaar bekeken kan worden welke situatie (A,B of C) voor de bewoner geldt. Situatie A (binnen effectgebied) en B (rand effectgebied) zijn de situatie die voornamelijk in aanmerking komen voor de VES-regeling. Situatie C (buiten effectgebied) niet.

Verwerking 2: Voorbereiden (KCDV)

Per aanvraag wordt bekeken of er een **nulmeting** zal worden uitgevoerd om de schades vast te leggen, of dat er zal worden gevraagd om **fotomateriaal** van de schades. Dit is afhankelijk van de locatie (a.d.h.v. trillingssterkte) en het bouwjaar van het schadeadres van de aanvraag.

Wanneer er geen nulmeting wordt gedaan, maar foto's worden opgevraagd, dient de aanvrager zelf dit fotomateriaal aan te leveren.

Bij een **nulmeting** gaat afdeling Planning een afspraak inplannen via Atabix.

Mocht er iets niet kloppen in de aanvraag of iets moet handmatig worden aangepast, dan wordt dit door afdeling Werkvoorbereiding bekeken. Ook als de foto's niet voldoen wordt dit door Werkvoorbereiding opgepakt en wordt een verzoek gedaan voor nieuwe foto's. Afwijzen gaat dus niet zomaar automatisch.

Verwerking 3: Aanvraag behandelen (KCDV)

Het IMG controleert of de aanvraag aan alle voorwaarden³ (zie onder 'Meer over de vaste vergoeding – waar moet uw aanvraag aan voldoen?') voldoet. En of het IMG nog wat aanvullende informatie van de aanvrager nodig heeft. Als dat zo is, krijgt aanvrager van het IMG bericht. Aanvrager kan deze informatie toevoegen aan zijn/haar 'Mijn dossier'.

Bij de optie **nulmeting** komt het IMG na het maken van een afspraak langs om foto's te maken van de schade.

Verwerking 4: Aanvraag afronden (beschikken) (BJZS)

Nadat de **nulmeting** is uitgevoerd en/of **foto's** zijn toegevoegd aan het dossier, kan het dossier in een Quality Assurance (QA) batch gezet worden. Vanuit deze batch vinden een aantal controles plaats (o.a. een foto controle).

Wanneer een QA batch is goedgekeurd krijgt de aanvrager de mogelijkheid een vaststellingsovereenkomst (VSO) te ondertekenen. Als hij/zij deze ondertekent wordt ingestemd met finaliteit⁴ (zie onder 'Meer over de vaste vergoeding – wat houdt dat in: een finale vergoeding?'). Tot het moment van ondertekenen kan de aanvrager de aanvraag intrekken. Daarna wordt (automatisch) het besluit gegenereerd en vindt uitbetaling plaats.

De aanvrager heeft nadien de mogelijkheid bezwaar in te dienen (zoals te doen gebruikelijk). Ongeacht de voorkeur van de aanvrager kan het besluit bij 'een papieren aanvraag' zowel per post als digitaal (mijn-dossier omgeving) worden verstuurd.

³ [Vaste vergoeding - Instituut Mijnbouwschade Groningen - Instituut Mijnbouwschade Groningen - Instituut Mijnbouwschade Groningen \(schadedoormijnbouw.nl\)](#)

⁴ [Vaste vergoeding - Instituut Mijnbouwschade Groningen - Instituut Mijnbouwschade Groningen - Instituut Mijnbouwschade Groningen \(schadedoormijnbouw.nl\)](#)

Verdere verwerking parallel aan het proces:**Afhandelen bezwaar (Bezwaar & Beroep) (BJZS)**

Verwerkt persoonsgegevens van de aanvragers bij het behandelen van bezwaren en beroepen van aanvragers tegen besluiten inzake de VES-regeling. Aangezien aanvragers kiezen voor de regeling en vooraf van de voorwaarden op de hoogte zijn, lijkt het onwaarschijnlijk dat deze afdeling veel met de VES-regeling te maken krijgt. Het is echter mogelijk dat een aanvrager zich binnen de bezwaartermijn bedenkt, en op komt tegen de beslissing op grond van de VES-regeling.

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.

Het doel van de VES-regeling is het besluiten op aanvragen tot vergoeding van schade en overlast ontstaan door beweging van de bodem als gevolg van de aanleg- of exploitatie van een mijnbouwwerk ten behoeve van het winnen van gas uit het Groningenveld of als gevolg van de gasopslag Norg.

De VES-regeling is een van de manieren waarop het IMG invulling geeft aan de aan hem opgedragen wettelijke plicht uit de Tijdelijke wet Groningen, artikel 2 lid 3 sub a en b, dan wel de taak van algemeen belang die hij uitvoert.

De VES-regeling biedt toegevoegde waarde ten opzichte van het reguliere schadeproces doordat aanvragen die slechts zien op een beperkte hoeveelheid schade, versneld en zonder opname kunnen worden afgehandeld. Niet alleen de aanvragers die gebruik maken van de VES-regeling krijgen zo sneller en eenvoudiger hun besluit, maar de VES-regeling zorgt er ook voor dat capaciteit vrij komt voor de overige dossiers.

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.

Verwerkingsverantwoordelijke: Instituut Mijnbouwschade Groningen.

Het Instituut Mijnbouwschade is een ZBO (zelfstandig bestuursorgaan), en valt dus niet onder de directe bevoegdheid van één van de ministeries. Het bestuur van het IMG stelt dus zelf het doel, de middelen, en de verwerkingen vast die hij in het kader van het uitoefenen van zijn bevoegdheden uitvoert.

Medewerkers van het Instituut hebben toegang tot de persoonsgegevens en het beeldmateriaal dat aanvragers leveren bij het doen van een aanvraag tot schadevergoeding.

Verwerkers:

- Atabix Solutions B.V. (in het geval van een nulmeting toegang tot de persoonsgegevens).
- Xerox (verwerken (versturen) adviesrapport, besluit, bijbehorende documentatie)
- DICTU (ICT)
- Auditdienst Rijk
- RVO (ondersteuning bij financiën, informatiemanagement, personeel conform dienstverleningsconvenant)

- Cyclomedia

Verstrekkers van persoonsgegevens:

- Aanvragers (vastgoedeigenaren, houders van appartementsrecht, opstalrecht, bekleemrecht of recht van erfpacht)
- Logius (DigiD)
- BRP
- Kadaster
- Commissie Mijnbouwschade (i.v.m. aanvraag bij verkeerde 'loket')
- NAM (Nederlandse Aardolie Maatschappij)

Ontvangers van persoonsgegevens

- Behandelend medewerkers van het IMG
- Auditdienst Rijk

Functionarissen (toegang tot de persoonsgegevens genoemd onder kopje 2)

- 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 het verwerken van de persoonsgegevens voor de VES-regeling is er in gelegen om eenvoudig een snel en gedegen besluit te kunnen nemen op de aanvraag tot schadevergoeding van aanvragers.

De VES-regeling biedt toegevoegde waarde ten opzichte van het reguliere schadeproces doordat aanvragen versneld en in de meeste gevallen zonder opname door deskundigen geautomatiseerd en digitaal kunnen worden afgehandeld. Niet alleen de aanvragers die gebruik maken van de VES-regeling krijgen zo sneller en eenvoudiger hun besluit, maar de VES-regeling zorgt er ook voor dat capaciteit vrij komt voor de overige dossiers.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

[Klik hier om infotekst te verbergen](#)

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

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

De verwerker Atabix Solutions B.V. is in Europa (Luxemburg) gevestigd. De servers bevinden zich in Duitsland (AWS). Atabix biedt en onderhoudt het tool voor de deskundigen. Als er geen **nulmeting** wordt uitgevoerd, dan heeft Atabix niets met de verwerking van doen.

Andere verwerkers:

- DICTU is gevestigd in Nederland en verwerkt uitsluitend in Nederland.
- Xerox is gevestigd in Nederland en verwerkt gegevens in Nederland.
- Auditdienst Rijk is gevestigd in Nederland en verwerkt gegevens in Nederland.
- RVO is gevestigd in Nederland en verwerkt gegevens in Nederland.
- Cyclomedia 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 besluiten bestaan ofwel uit het afwijzen van de aanvraag in het geval er niet aan de voorwaarden wordt voldaan, of het toewijzen van de aanvraag en het uitkeren van precies € 5.000,-. Een inhoudelijke beoordeling hoeft dus niet meer te worden uitgevoerd, als eenmaal is komen vast te staan dat er sprake is van enige schade (zichtbare schade op minimaal 1 foto) en aan de overige voorwaarden wordt voldaan.

Per aanvraag wordt er wel een keuze gemaakt door het IMG of er een nulmeting zal worden uitgevoerd om de schades vast te leggen, of dat er zal worden gevraagd om fotomateriaal van de schades. Dit is afhankelijk van de locatie en het bouwjaar van het schadeadres van de aanvraag. Wanneer er geen nulmeting wordt gedaan, maar foto's worden opgevraagd, dient de aanvrager zelf dit fotomateriaal aan te leveren. Het fotomateriaal zal in eerste instantie nog integraal worden getoetst door medewerkers. Op een later moment zal dit worden teruggebracht naar steekproefsgewijze controle wanneer de resultaten daartoe aanleiding geven.

Volgens het projectteam is het huidige beeld dat minder dan 1 promille van de foto's vragen oproepen en aanleiding geven tot het vragen van opheldering of nieuwe foto's. Een grondigere evaluatie volgt nog. Wanneer het risico van aanlevering van onjuiste foto's gering is kan worden overgegaan op een nog vast te stellen steekproef.

De filter die wordt genoemd is de geautomatiseerde check die momenteel wordt ontwikkeld zoals genoemd in de volgende paragraaf. Foto's waarop geen schade te zien is leiden dan tot uitval en daarmee tot beoordeling door mensenogen.

Geautomatiseerde individuele besluitvorming

Op den duur is het echter de bedoeling om door gebruik van een systeem van automatische beeldherkenning vast te stellen of er schades zichtbaar zijn op het aangeleverde fotomateriaal. Op dat moment is er sprake van geautomatiseerde individuele besluitvorming (artikel 22 AVG) voor de gevallen waar geen nulmeting wordt verricht. Er is dan immers geen medewerker meer die het besluit beïnvloedt. Hierbij wordt echter opgemerkt dat bij de ontwikkeling van beeldherkenning voor VES door het ontwikkelteam van KPMG is benadrukt dat de beeldherkenning dient ter ondersteuning van het proces, en nooit als een op zichzelf staande tool gebruikt kan worden.⁵ Reden hiervoor is dat de menselijk maat behouden moet blijven in het proces. Beeldherkenning kan volgens het ontwikkelteam bijdragen aan het proces, maar moet de regeling niet dicteren. Daarnaast is bij de ontwikkeling rekening gehouden met een 'human in the loop' voor een optimale werking van beeldherkenning.

Geautomatiseerde besluitvorming wordt verboden door artikel 22 lid 1 van de AVG, wanneer het besluit in kwestie rechtsgevolgen heeft voor de betrokkene. We kunnen aannemen dat dat het geval is, aangezien de aanvrager bij een positief besluit recht heeft op € 5.000,- en bij een negatief besluit niet. Een beroep op één van de uitzonderingen van lid 2, sub a t/m c, lijkt buiten bereik, gezien geen van deze leden van toepassing is op de situatie. In deze DPIA wordt volstaan met de constatering dat er geen sprake is van de totstandkoming van een overeenkomst (art. 22 lid 2 sub a AVG) en dat de besluitvorming niet is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepaling (art. 22 lid 2 sub b AVG). De uitzonderingsgrond toestemming van art. 22 lid 2 sub c AVG gaat in dit geval niet op aangezien er tussen het IMG en de aanvrager een zekere machtsverhouding bestaat die op gespannen voet staat met de *vrijelijk* gegeven toestemming (overweging 43 van de AVG).

Omdat de geautomatiseerde individuele besluitvorming op grond van artikel 22 lid 1 AVG wordt verboden en de uitzonderingen van artikel 22 lid 2 AVG niet van toepassing zijn, kan enkel art. 40 UAVG het verbod tot geautomatiseerde individuele besluitvorming opheffen. In art. 40 lid 1

⁵ Blijkt uit de meeting van 8 maart 2022 olv **5.1.2e** met IB&P, waarin KPMG de uitlegbaarheid en transparantie van beeldherkenning heeft besproken.

UAVG staat dat het verbod tot geautomatiseerde individuele besluitvorming niet geldt wanneer dit noodzakelijk is voor het voldoen aan een wettelijke verplichting. Deze noodzakelijkheid blijkt echter niet uit de regeling, omdat de regeling momenteel volledig handmatig wordt uitgevoerd. Automatisering van het proces met het gebruik van beeldherkenning is enkel aantrekkelijk voor de snelle doorlooptijd van de besluiten en het voorkomt tijdbesteding aan 'geestdodend werk'.⁶ Art. 40 UAVG kan daarom geen uitzonderingsgrond bieden voor geautomatiseerde individuele besluitvorming in het kader van de VES-regeling.

Het geheel uitsluiten van menselijke besluitvorming of de beperking hiervan tot dreigend negatieve besluiten in het proces van VES wordt om bovenstaande redenen ten zeerste afgeraden. Indien op een later moment wordt besloten om geautomatiseerde individuele besluitvorming toe te passen dient deze DPIA te worden aangevuld of een nieuwe DPIA te worden uitgevoerd.

Kwaliteit van de gegevens en discriminatie

Indien op een later moment wel wordt gekozen voor het toepassen van beeldherkenning dient rekening te worden gehouden met het volgende. Het huidige beeldherkenningsmodel wordt getraind op basis van foto's afkomstig uit dossiers van de regeling fysieke schade. Omdat het gebied van de VES-regeling de randen van het aardbevingsgebied betreffen is het denkbaar dat de schade kleiner is en daardoor minder goed zichtbaar. Het is onduidelijk in hoeverre er bij het trainen van het beeldherkenningsmodel rekening is gehouden met de minder goede zichtbaarheid van (kleinere) schades die wel degelijk onder de VES-regeling vallen en in hoeverre de beeldherkenningssoftware deze schade kan herkennen. Het is niet duidelijk welke foutmarge voor de beeldherkenningssoftware als acceptabel wordt beschouwd. Uit de meest recente informatie van het ontwikkelteam blijkt dat de huidige accuraatheid 86% is.

Daarnaast is het onduidelijk welke invloed de apparatuur van de aanvrager heeft op het verloop van de aanvraag. De op het oog zichtbare schade kan onduidelijk op de foto komen door lichtinval, het materiaal waar de schade zich bevindt of het type object van de schade. Het beeldherkenningsmodel wordt getraind met foto's van schade op diverse materialen en gebouwenkenmerken, waarbij de foto's zijn gemaakt door deskundigen. Het is onbekend in hoeverre de schade wordt herkend indien de foto is gemaakt door een slechte kwaliteit of sterk verouderde camera. Dit is relevant voor het voorkomen van discriminatie. Elke aanvrager, ongeacht de economische achtergrond, dient gelijk behandeld te worden in de aanvraag. Verslechterde of verouderde apparatuur en daardoor onduidelijke foto's mogen niet leiden tot een false-negative door de beeldherkenningstool. *Risico: verslechterde of verouderde apparatuur en daardoor onduidelijke foto's kunnen leiden tot een false-negative door de beeldherkenningstool, waardoor (onbedoeld) sprake is van discriminatie.*

Menselijke tussenkomst

Er kan voorkomen worden dat er sprake is van volledig geautomatiseerde individuele besluitvorming bij het gebruik van beeldherkenning wanneer er menselijke tussenkomst is voordat er een besluit tot stand komt (artikel 22 lid 3). De menselijke tussenkomst is vereist bij zowel een positief besluit (€5.000 wordt toegekend) als een negatief besluit (er wordt niet aan de voorwaarden voldaan, €5.000 wordt niet toegekend).

Volgens de Memorie van Toelichting, p. 120, bestaat er geen bezwaar tegen het gebruik van geautomatiseerde processen als onderdeel van het proces dat aan de besluitvorming zelf voorafgaat.⁷ Beeldherkenning in combinatie met VES is dus mogelijk, maar enkel wanneer

⁶ Mail van projectteam "RE: VES – DPIA, beeldherkenning en fraude" van 17-02-2022.

⁷ Kamerstuk 34851, nr. 3 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl) p. 120.

menselijke tussenkomst in het proces bestaat. Voorwaarde hieraan is dat de menselijke tussenkomst werkelijk verschil kan maken in het besluitvormingsproces. Een enkele controle op de aanvraag of een persoon die op de knop "afronden" klikt is hiervoor dus niet voldoende. De medewerker moet het proces en de uitkomst kunnen beïnvloeden om te kunnen spreken van menselijke tussenkomst. Op die wijze kan beeldherkenning in combinatie met menselijke tussenkomst een uitkomst bieden om het proces VES achter de schermen te versnellen.

Kwaliteit van (persoons)gegevens, integriteit en fraude

In de regeling VES (eventueel in combinatie met beeldherkenning) wordt enkel gekeken of er schade zichtbaar is op de door de aanvrager of gemachtigde ingestuurde foto's. Er wordt door medewerkers of beeldherkenningssoftware niet gekeken of de foto's reeds bij het IMG bekend zijn of werkelijk bij het desbetreffende pand horen. De fotocontrole is momenteel (maart 2022) handmatig en het is uiterst onwaarschijnlijk dat herkend zal worden dat een foto eerder is gebruikt. Automatische beeldherkenning zal hier vooralsnog niet op toetsen. Aanvragers of gemachtigden zouden foto's kunnen maken in de woning van derden en de schade kunnen afdoen als horende bij het betreffende pand. Tevens zouden aanvragers of gemachtigden foto's van Google of andere (openbare) webpagina's kunnen halen van objecten met schade.

Indien foto's toch als niet-afkomstig van het betreffende pand herkend worden, zal de aanvrager of gemachtigde worden benaderd met het verzoek om toelichting of nieuwe foto's te sturen. Het is momenteel niet te zeggen of het gebruik van foto's die niet afkomstig zijn van het pand leiden tot afwijzing, verder onderzoek of tot onderzoek naar de aanvraag/aanvragen waar de foto's eerder zijn gebruikt. Het is daardoor niet op voorhand bekend of het gebruik van deze foto's zal leiden tot terugvordering van de schade, aangifte van fraude of andere maatregelen. Of en in hoeverre de verhouding tussen de aanvrager en gemachtigde hierin worden onderzocht en meegewogen is onduidelijk. Het risico bestaat dat er onterecht schade wordt uitgekeerd of onterechte terugvorderingen worden gedaan.

5.1.2i

Profilering & big data

Verder kan op grond van bovenstaande kan worden vastgesteld dat er geen gebruik wordt gemaakt van profilering. En er geen sprake is van gegevensverwerking die als 'big data' valt te classificeren.

Metadata

Met het uploaden van de foto's door de aanvragers wordt metadata met de foto's geupload. In principe wordt er niets met de metadata gedaan, waardoor de metadata door het IMG worden verwerkt (opgeslagen).

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. De VES-regeling is net als de reguliere schade afhandeling gestoeld op artikel 2 lid 3 sub a en b.

De spelregels voor de VES en de werkwijze van het IMG bestaan verder uit beleidsregels⁸. Zowel de zelf vastgestelde werkwijze van het Instituut als de regels voor de VES zijn beide terug te vinden op de website van het IMG.

Voor het verwerken van het BSN geldt specifieke regelgeving, zie daarvoor het antwoord onder 12.

Tevens is onder andere de volgende wetgeving van toepassing:

- Archiefwet
- Algemene Wet Bestuursrecht
- Wet openbaarheid van bestuur (Wob) - per 1 mei 2022 - Wet open overheid (Woo)
- Wet basisregistratie personen
- Wet algemene bepalingen burgerservicenummer
- Informatiebeveiligings- en privacybeleid IMG

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

⁸ [Werkwijze \(schadedoormijnbouw.nl\)](#)

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 (zie bijlage 3), aangemerkt als 'hotspot', waarbij de persoonsgegevens worden 'gearchiverd 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.

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.

Artikel 6 lid 1 sub c AVG. Artikel 2 lid 3 sub a en b dragen aan het IMG een wettelijke plicht op om de schadevergoeding af te handelen, en bieden daarmee ook een wettelijke grondslag voor het Instituut om gegevens te verwerken voor zover dat past binnen het doel van de afhandeling van de schadevergoeding.

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:

- a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
- b. 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;
- c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
 - d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
 - e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
 - f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
 - g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
 - h. 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;
 - i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
 - j. 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.

Strafrechtelijke persoonsgegevens worden niet verwerkt.

Bij de VES-regeling worden in principe ook geen bijzondere persoonsgegevens verwerkt. Wel vormt het onderdeel waarbij aanvragers zelf fotomateriaal aanleveren als onderbouwing voor hun aanvraag een zeker risico, aangezien het denkbaar is dat een aanvrager per abuis materiaal aanlevert waaruit bepaalde bijzondere persoonsgegevens kunnen worden afgeleid. Een voorbeeld daarvan is dat men bijvoorbeeld een overzichtsfoto levert met een traplift daarop zichtbaar, waaruit gegevens over de medische toestand van een aanvrager kunnen worden afgeleid. Hiervoor zijn foto instructies op de website geplaatst.

Voor de VES-regeling wordt net als bij de reguliere fysieke schaderegeling het BSN of 'nationaal identificatienummer' verwerkt. De regels voor het gebruik van dit nummer zijn terug te vinden in artikel 87 van de AVG en artikel 46 van de Uitvoeringswet AVG. Op grond van artikel 10 van de Wet algemene bepalingen Burgerservicenummer mogen overheidsorganen het BSN verwerken in het kader van hun bevoegdheden. Het IMG geeft door middel van de VES-regeling invulling aan zijn taak van het afhandelen van de schade als gevolg van de gaswinning, en voor die taak mag verwerking van het BSN dus worden ingezet.

13. Doelbinding



Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel 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:

- a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenoemde verdere verwerking;
- b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;

- c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- e. 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:

- a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- b. 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 persoonsgegevens worden verwerkt voor hetzelfde doel als waarvoor deze worden verzameld.

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?.**

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken. Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechttoets van het IAK.

a. Er is voldaan aan het vereiste van proportionaliteit.

Het doel om burgers die schade hebben ondervonden van de gaswinning uit het Groningenveld ruimhartig en voortvarend te compenseren is de laatste jaren een belangrijk speerpunt geweest in het beleid van de regering. Daarnaast is het voortdurend onderwerp van media-aandacht en maatschappelijke discussie, waarbij er een sterk gevoelde roep leeft om recht te doen aan de getroffen. Daarmee valt te stellen dat het doel van het op een rechtvaardige manier afwikkelen van de schade van de gaswinningen een onderwerp van eminent belang is.

De VES-regeling levert een belangrijke bijdrage aan de voortvarendheid van de schade afhandeling. Doordat een inhoudelijke beoordeling van de schade achterwege kan blijven in dossiers waarin voor een vaste vergoeding wordt gekozen, wordt capaciteit vrijgespeeld van deskundigen en medewerkers, die vervolgens kan worden ingezet op de ingewikkelder dossiers, zodat in de behandeling van die dossiers een versnelling kan worden gerealiseerd.

Daarnaast brengt de regeling meer balans in de verhouding tussen kosten die moeten worden gemaakt om de schade vast te stellen, ten opzichte van de hoeveelheid geld die uiteindelijk wordt uitgekeerd aan de gedupeerden. Het feit dat er geen deskundigenadvies hoeft te worden ingewonnen betekent immers niet alleen dat er meer capaciteit van deskundigen overblijft voor andere dossiers, maar ook dat er voor deze dossiers minder kosten worden gemaakt om ze af te handelen.

Aangezien de gegevensverzameling van de VES-regeling voor het grootste deel identiek is aan het reguliere schadeproces, wordt verwezen naar de DPIA van dit onderwerp voor een weging van de proportionaliteit van de gegevensbescherming.

Punten waarin de VES-regeling echter afwijkt van de reguliere schadeprocedure zijn het semi-geautomatiseerde besluitvormingsproces en het gebruik van beeldherkenning om na te gaan of er sprake is van schade op het aangeleverde fotomateriaal. Daarbij speelt dat er een zeer groot aantal potentiële aanvragers een beroep zouden kunnen doen op de regeling, tot aan 200.000.

b. Er is voldaan aan het vereiste van subsidiariteit.

De verwerkingsdoeleinden worden op de minst nadelige wijze verwerkt. Alleen de (persoons)gegevens die minimaal nodig zijn om de schade af te kunnen handelen worden

verwerkt. Daarbij is 1 foto waarop schade zichtbaar is voldoende.
Verder zijn de NAW-gegevens van de betrokkene van belang om te kunnen vaststellen om welke persoon en adres het gaat en of de aanvrager eigenaar is van het pand. Met Kadasterdata en BRP-gegevens worden deze gegevens opgehaald en/of geverifieerd.
De andere gegevens zijn noodzakelijk voor de uitbetaling van de schade.

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 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.

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

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 privacyregelgeving 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.

Zie bijlage – Risico register

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.

Zie bijlage – Risico register

Bijlage Risico register

	Risico	Gevolgen	Maatregel	Actiehouder	Status	Einddatum
1	Geen (proces)eigenaar voor de VES regeling vastgesteld.	Niet duidelijk wie verantwoordelijk is voor de uitvoering van de DPIA VES en de daaraan gekoppelde (risico's en) maatregelen.	Vaststellen wie verantwoordelijk is voor de DPIA VES en de aan hen toegewezen maatregelen.	MT	Nog uit te voeren	1-6-2022
2	Rechtstreeks uploaden van foto's van de gebruiker naar het IMG --> beveiligingsrisico's en ontbreken filter.	Illegale content --> het aanwezig hebben van strafrechtelijk verboden beeldmateriaal. Of auteurs rechtelijk beschermd werken. Of anderszins onrechtmatige content.	Opstellen protocol om illegale content bij het uploaden van foto's te voorkomen.	Proceseigenaar	Nog uit te voeren	1-6-2022
3	Rechtstreeks uploaden van foto's van de gebruiker naar het IMG --> beveiligingsrisico's en ontbreken filter.	Geen goede kwaliteit van de persoonsgegevens en daarmee de integriteit van de aanvraag.	Een nadere onderbouwing van hoe de kwaliteit van de persoonsgegevens wordt gewaarborgd.	Proceseigenaar	Nog uit te voeren	1-6-2022

5.1.2i

5	De procesbeschrijving(en) bij de VES regeling zijn nog niet volledig beschreven dan wel vastgesteld door de proceseigenaar.	Doordat de processen niet goed zijn beschreven is er mogelijk geen juiste procesgang, waardoor aanvragen buiten het proces worden behandeld.	Er dient een procesbeschrijving te komen voor: - VES Indienen en Registreren, Vorbereiden, Plannen en Schade opnemen - VES Vorbereiden besluit en Beoordelen besluit En deze procesbeschrijvingen dienen definitief te zijn.	Proceseigenaar	Nog uit te voeren	1-6-2022
6	Cyclomedia wordt ingeschakeld bij de VES regeling. Daarbij wordt waardevolle data uit geavanceerd beeldmateriaal gehaald.	Niet bekend wat Cyclomedia binnen de regeling VES precies doet. En welke afspraken er zijn gemaakt rondom gegevensverwerking.	Een nadere onderbouwing van wat de rol van Cyclomedia is in relatie tot de VES regeling? En welke afspraken zijn er met deze partij gemaakt?	Proceseigenaar	Nog uit te voeren	1-6-2022

7	Er is geen duidelijke definitie van de rollen en verantwoordelijkheden vastgesteld, hetgeen kan leiden tot onrechtmatige toegang tot persoonsgegevens van de aanvrager en ten koste kan gaan van de waarborging van persoonsgegevens.	Hierdoor is de kans dat onbevoegden toegang hebben tot persoonsgegevens van aanvragers en mogelijk hier misbruik van maken.	Controleren of de autorisatiematrix bij fysieke schade aan gebouwen en werken nog juist is.	Proceseigenaar	Nog uit te voeren	1-6-2022
8	Persoonsgegevens worden (onrechtmatig) langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze is verzameld.	Het IMG heeft geen gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens.	Er dient een gedocumenteerd bewaarbeleid en verwijderingsprocedures ten aanzien van persoonsgegevens worden opgesteld.	Proceseigenaar	Nog uit te voeren	1-6-2022
9	Onvoldoende inzicht in de schadeopname app.	Vanuit privacy geen inzicht in de schadeopname app, waardoor mogelijk de rechten en vrijheden van aanvragers in het geding komen.	Aan het projectteam om meer inzicht te geven in de schadeopname app in relatie tot de VES regeling.	Proceseigenaar	Nog uit te voeren	1-6-2022
10	Gebruik van ondeugdelijk mobiele devices (apparatuur).	Verslechterde of verouderde apparatuur en daardoor onduidelijke foto's kunnen leiden tot een false-negative door de beeldherkenningstool, waardoor (onbedoeld) sprake is van discriminatie.	Het model beter trainen. Of gebruik maken van het menselijk oog.	Proceseigenaar	Nog uit te voeren	1-6-2022
11	Verkrijgen van bepaalde bijzondere persoonsgegevens door aanvrager zelf.	Het door de aanvrager aanleveren van eigen fotomateriaal als onderbouwing voor hun aanvraag, waarbij mogelijk bepaalde bijzondere persoonsgegevens kunnen worden afgeleid. Niet duidelijk of er foto instructies zijn voor het blurren of verwijderen van bijzondere persoonsgegevens.	In het protocol VES opnemen dat bijzondere persoonsgegevens geblurd of verwijderd worden uit de aanvraag.	Proceseigenaar	Nog uit te voeren	1-6-2022

5.1.2i

13	Criteria voor goede foto's zijn onduidelijk.	Kans dat daardoor de foto's niet voldoende zijn.	Protocol opstellen voor juiste foto's en de aanvrager hierin begeleiden.	Proceseigenaar	Nog uit te voeren	1-6-2022
14	Bij geautomatiseerde individuele besluitvorming zal beeldherkenning worden gebruikt als op zichzelf staande tool i.p.v. ondersteuning zoals bedoeld door het ontwikkelteam.	De kwaliteit van de uitkomsten door de software is daardoor onzeker.	Houd altijd een 'human in the loop' of pas de 'use case' van beeldherkenning aan bij geautomatiseerde besluitvorming.	Proceseigenaar	Nog uit te voeren	1-6-2022
15	Geen goede onderbouwing waarom geautomatiseerde besluitvorming wordt gebruikt bij de VES regeling.	De noodzakelijkheid van de geautomatiseerde besluitvorming is niet aangetoond. Dit kan gevolgen hebben voor aanvragers die hun rechten en vrijheden niet kunnen uitoefenen. Bij geautomatiseerde besluitvorming vraagt om een nieuwe DPIA.	Indien op een later moment wordt besloten om geautomatiseerde individuele besluitvorming toe te passen dient deze DPIA te worden aangevuld of een nieuwe DPIA te worden uitgevoerd.	Proceseigenaar	Nog uit te voeren	1-6-2022
16	Het is onduidelijk in hoeverre de beeldherkenningstool juist getraind en toegepast kan wordend op minder duidelijk zichtbare schade.	Gevolg dat uit de meest recente informatie van het ontwikkelteam blijkt dat de huidige accuraatheid maar 86% is.	"Use case" aanpassen en het model in dat geval beter trainen!	Proceseigenaar	Nog uit te voeren	1-6-2022
17	Er is nog geen besluit genomen over de rol van beeldherkenning bij VES.	Gevolg het verplicht uitvoeren van een aanvullende DPIA.	Een nadere onderbouwing welke rol beeldherkenning bij de VES regeling krijgt.	Proceseigenaar	Nog uit te voeren	1-6-2022
18	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.	Proceseigenaar	Nog uit te voeren	1-6-2022



Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond.
Met open vizier