Gegevensbeschermingsbeleid @ VITO

Beleidsdocument

Hoofdstuk I - Kader en scope

In dit gegevensbeschermingsbeleid wordt het beleid dat de Vlaamse Instelling voor Technologisch Onderzoek (VITO) hanteert bij de bescherming en verwerking van persoonsgegevens beschreven.

1. Wettelijke kader

De bescherming van persoonsgegevens is een grondrecht dat in het Handvest van de grondrechten van de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is vastgelegd. De Algemene Verordening Gegevensbescherming ('Verordening') is een Europese wet die de bescherming van dit grondrecht regelt (de officiële benaming is 'General Data Protection Regulation' ook wel 'GDPR').

De Verordening is vanaf 25 mei 2016 in werking getreden en is vanaf 25 mei 2018 rechtstreeks toepasselijk in de hele Europese Unie.

Bij het invullen en uitvoeren van zijn gegevensbeschermingsbeleid en de omgang met persoonsgegevens houdt VITO rekening met:

- de GDPR die de rechtmatige en zorgvuldige omgang met persoonsgegevens binnen de Europese Unie regelt;
- de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens gepubliceerd op 5 september 2018.

VITO hanteert in het kader van dit gegevensbeschermingsbeleid en bij zijn verwerking van persoonsgegevens dezelfde begripsbepalingen als vastgelegd in de GDPR dan wel in overige van toepassing zijnde wetgeving.

2. Autoriteit

2.1 Vlaamse Toezichtscommissie

De Vlaamse Toezichtscommissie ("VTC") is als Vlaamse gegevensbeschermingsautoriteit bevoegd voor Vlaamse overheden/instanties. Aangezien VITO valt onder de definitie van Vlaamse openbare instelling, zal de Vlaamse Toezichtscommissie voor een aantal zaken bevoegd zijn. Zo zal VITO datalekken melden bij de VTC en zal de VTC bevoegd zijn om eventuele klachten van betrokkenen te behandelen. Daarnaast zal de VTC in het kader van protocollen, die VITO afsluit met andere Vlaamse overheden/instanties, bevoegd zijn.

2.2 Gegevensbeschermingsautoriteit

De Gegevensbeschermingsautoriteit ("GBA") is de Belgische gegevensbeschermingsautoriteit die in het algemeen bevoegd is voor de naleving van de grondbeginselen van bescherming van persoonsgegevens. Zij blijft steeds bevoegd om klachten van betrokkenen te behandelen.

3. Doel gegevensbeschermingsbeleid

Als strategisch onderzoekscentrum voert VITO onderzoeksprojecten uit, samen of in opdracht met andere kennisinstellingen, overheden en/of bedrijven. In het kader van deze samenwerking en dienstverlening aan of ten behoeve van opdrachtgevers, externe partijen en klanten verwerkt VITO persoonsgegevens. Ook van zijn medewerkers en overige voor hem werkzaam zijnde personen verwerkt VITO persoonsgegevens. Tenslotte verwerkt VITO ook persoonsgegevens van bezoekers van zijn website(s).

VITO hecht grote waarde aan een rechtmatige, behoorlijke, transparante en daarmee kwalitatieve verwerking van persoonsgegevens. VITO wil vertrouwen bieden aan zijn opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen in de wijze waarop VITO met hun persoonsgegevens en privacy omgaat en stelt zich een zorgvuldige bescherming en verwerking van persoonsgegevens ten doel.

Met dit gegevensbeschermingsbeleid wil VITO eveneens werken aan een bewustwording op het waarborgen gegevensbescherming.

4. Toepassingsgebied gegevensbeschermingsbeleid

Het gegevensbeschermingsbeleid van VITO is van toepassing op:

- de hele VITO-organisatie, d.w.z. alle interne en externe medewerkers alsmede overige personen die voor VITO werkzaam zijn;

- alle processen en procedures inzake verwerking van persoonsgegevens die VITO voor zijn opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen uitvoert;
- alle ondersteunende diensten en units van VITO; en
- alle verwerkingsactiviteiten en gegevensverzamelingen van persoonsgegevens die door of namens VITO worden verricht.

5. Bestuur gegevensbeschermingsbeleid

Vanuit de grote waarde die VITO hecht aan een zorgvuldige en adequate bescherming en verwerking van persoonsgegevens, acht VITO het essentieel dat er een efficiënt en effectief bestuur met betrekking tot privacy wordt ingericht.

5.1 Centrale inrichting

De Raad van bestuur van VITO is (eind)verantwoordelijk voor een zorgvuldige en juiste naleving van de privacy wet- en regelgeving.

Binnen VITO is het toezicht op de bescherming van de privacy en de verwerking van persoonsgegevens toebedeeld aan de Data Protection Officer (DPO).

Een DPO is een wettelijk gereguleerde functionaris die:

- informeert en adviseert over de privacy verplichtingen;
- toezicht houdt op de toepassing en naleving van de privacy wet- en regelgeving en dit gegevensbeschermingsbeleid;
- advies verstrekt over de effectenbeoordeling gegevensbescherming en toeziet op de uitvoering ervan;
- het contact onderhoudt met de toezichthoudende autoriteit, de Vlaamse Toezichtscommissie; en
- rapporteert aan de raad van bestuur van VITO.

In de situaties waarin VITO als verwerker optreedt, informeert of rapporteert de DPO conform de met de opdrachtgevers hierover gemaakte afspraken over de toepassing en naleving van de privacy wet- en regelgeving en dit gegevensbeschermingsbeleid door VITO in relatie tot de gegevensverwerkingen die de opdrachtgever aan VITO heeft uitbesteed.

VITO zorgt ervoor dat:

- de DPO naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- de DPO wordt ondersteund met bevoegdheden en middelen om zijn taken te kunnen vervullen en zijn deskundigheid in stand te kunnen houden;
- de DPO zijn rol onafhankelijk kan vervullen;
- de DPO geen nadeel ondervindt bij de uitvoering van zijn taken;
- betrokkenen contact kunnen opnemen met de DPO over hun gegevensverwerkingen en de uitvoering van hun rechten;
- de DPO geen andere taken en plichten binnen VITO vervult die leiden tot een belangenconflict.

Deze functionaris is aangemeld bij de Vlaamse Toezichtscommissie.

5.2 Decentrale inrichting

Voor de units of ondersteunende diensten van VITO zijn de desbetreffende unitmanagers of directieleden verantwoordelijk voor een zorgvuldige en juiste naleving van de privacy wet- en regelgeving door hun respectievelijke dienst.

Binnen de units en ondersteunende diensten zijn specifieke functionarissen, GDPR-verantwoordelijken, aangewezen die erop toezien dat effectieve en efficiënte processen op privacy en verwerking van persoonsgegevens worden ingericht en de externe en interne privacyregels worden nageleefd. Zij rapporteren hierover aan de DPO, zodat deze zijn taken zoals beschreven zorgvuldig en naar behoren kan uitvoeren.

Door de units en ondersteunende diensten worden in het kader van deze interne beheersing specifieke op privacy en het verwerken van persoonsgegevens afgestemde controlemaatregelen uitgevoerd. De DPO wordt door de units en ondersteunende diensten geïnformeerd over de (controle)bevindingen op privacy en de verwerking van persoonsgegevens.

Hoofdstuk II - Verwerkingsbeginselen

Iedere verwerking van persoonsgegevens moet voldoen aan de in dit hoofdstuk vermelde verwerkingsbeginselen. Deze verwerkingsbeginselen vormen het normatieve kader van het gegevensbeschermingsbeleid. Zij worden nader geconcretiseerd in verplichtingen die VITO heeft om deze gegevensverwerkingen zorgvuldig en naar behoren uit te voeren om daarmee te voldoen aan de eisen en verplichtingen die de privacy wet- en regelgeving stellen en de rechten die opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen ten aanzien van de verwerking van hun persoonsgegevens door VITO hebben.

1. Uitgangspunten

1.1 Rechtmatigheid, behoorlijkheid en transparantie

VITO verwerkt persoonsgegevens alleen voor gerechtvaardigde doeleinden en draagt er zorgt voor dat de verwerking netjes en op verantwoorde wijze gebeurt. Ook maakt VITO duidelijk voor welke doelen en op welke wijze persoonsgegevens worden verwerkt.

1.2 Doelbinding

VITO verzamelt persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De gegevens worden alleen voor een ander doel gebruikt als dat doel niet onverenigbaar is met de oorspronkelijke verzameldoeleinden.

1.3 Dataminimalisatie

VITO verwerkt alleen persoonsgegevens die toereikend, ter zake dienend en noodzakelijk zijn voor de doeleinden waarvoor ze worden verwerkt. Dit betekent dat VITO zich beperkt tot een minimale gegevensverwerking.

1.4 Juistheid

VITO draagt er zorgt voor dat de persoonsgegevens juist en actueel zijn en neemt alle redelijke maatregelen opdat gegevens die dat niet (meer) zijn, worden gewist of gerectificeerd.

1.5 Opslagbeperking

VITO bewaart persoonsgegevens niet langer in een identificeerbare vorm dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.

1.6 Integriteit en vertrouwelijkheid

VITO neemt passende technische en organisatorische maatregelen om te waarborgen dat de persoonsgegevens passend zijn beveiligd. De persoonsgegevens worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Een belangrijke maatregel om dit te waarborgen betreft de procedure voor het melden van datalekken.

2. Verwerkingsgrondslagen

Elke gegevensverwerking moet gerechtvaardigd zijn. Om gerechtvaardigd te zijn moet de verwerking te baseren zijn op tenminste een van de in de GDPR vastgelegde rechtsgrondslagen. Of een rechtsgrondslag relevant is hangt onder meer af van het doel dat met de gegevensverwerking wordt beoogd.

De (meest) relevante rechtsgrondslagen voor VITO zijn:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op VITO rust; of
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van VITO of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van de persoonsgegevens nopen, zwaarder wegen dan die belangen.

Bij de noodzakelijkheidsgrondslagen maakt VITO de afweging of de verwerkingen noodzakelijk en daarmee gerechtvaardigd zijn voor de in deze grondslagen genoemde doeleinden. Hierbij wordt gekeken of de verwerking van gegevens proportioneel is en of zij voldoet aan de eis van subsidiariteit.

De vraag of de verwerking proportioneel is, beoordeelt VITO aan de hand van de criteria van effectiviteit en

evenredigheid. Een verwerking is effectief als met de gegevensverwerking het gesteld doel kan worden bereikt of als dat zeer waarschijnlijk is. Een verwerking is evenredig als het doel dat met de verwerking wordt nagestreefd in verhouding staat tot het feit dat persoonsgegevens worden verwerkt.

Bij de vraag of de verwerking subsidiair is, kijkt VITO of het doel niet op een andere, minder ingrijpende wijze kan worden bereikt.

Alleen als de gegevensverwerking niet te baseren valt op een van de noodzakelijkheidsgrondslagen, is toestemming van de betrokkene voor de gegevensverwerking nodig. Ook een verwerking op de grondslag toestemming moet voldoen aan de eisen van proportionaliteit en subsidiariteit.

De verwerkingsgrondslagen die VITO hanteert in het kader van specifieke verwerkingen worden vastgelegd in het verwerkingsregister.

3. Verwerkingsverantwoordelijke - Verwerker

VITO verwerkt persoonsgegevens als verwerkingsverantwoordelijke, maar ook als verwerker. In welke hoedanigheid VITO deze gegevens verwerkt, hangt af van de aard van zijn bedrijfsvoering en dienstverlening alsook van zijn juridische bevoegdheid of positie ten opzichte van de gegevensverwerking.

De mate waarin of de wijze waarop de privacy verplichtingen van toepassing zijn, is afhankelijk van de rol en functie die VITO heeft ten aanzien van de verwerking van persoonsgegevens. De privacy wet- en regelgeving legt aan een verwerkingsverantwoordelijke meer omvattende, zwaardere en strakkere verplichtingen op dan aan een verwerker. Ten gronde is en blijft de verwerkingsverantwoordelijke verantwoordelijk voor de gegevensverwerking door de verwerker. Althans in zoverre de verwerker verwerkingsactiviteiten verricht in opdracht van en ten behoeve van de verwerkingsverantwoordelijke.

3.1 Verwerkingsverantwoordelijke

VITO is verwerkingsverantwoordelijke voor alle verwerkingen van persoonsgegevens waarvan VITO bepaalt welke persoonsgegevens worden verwerkt, voor welk doel dit gebeurt en met welke middelen dit plaatsvindt.

Wanneer VITO samen met anderen, zoals opdrachtgevers en externe partijen, het doel van en middelen voor de gegevensverwerking bepaalt, kan er sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. Of hiervan sprake is, hangt in belangrijke mate af van de juridische verhoudingen tot en de contractuele afspraken (de jure) met die opdrachtgevers en externe partijen. De facto moet worden nagegaan welke feitelijke invloed heeft VITO op de gegevensverwerking.

3.2 Verwerker

VITO is verwerker wanneer hij ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder dat hij aan diens rechtstreekse gezag is onderworpen of in een hiërarchische verhouding tot die verwerkingsverantwoordelijke staat.

Het moet hier gaan om gegevensverwerking die in opdracht aan VITO is gegeven en waar de dienstverlening van VITO volledig gericht is op het uitvoering geven aan die opdracht.

De rol die VITO opneemt in het kader van specifieke verwerkingen wordt vastgelegd in het verwerkingsregister alsook in de (verwerkings-)overeenkomsten die met derden hiertoe worden gesloten.

4. Bijzondere situaties

In deze paragraaf zijn een aantal bijzondere situaties met betrekking tot het verwerken van persoonsgegevens opgenomen waar VITO in zijn bedrijfsvoering en bij zijn dienstverlening meer dan incidenteel mee te maken krijgt of kan krijgen en waarvan het essentieel en relevant is dat VITO daar beleid over voert.

4.1 Toestemming

Een van de rechtsgrondslagen voor een gerechtvaardigde gegevensverwerking is toestemming.

Er is sprake van geldige toestemming als deze:

- vrij gegeven is en betrokkene de vrije keuze heeft te weigeren;
- specifiek en geïnformeerd is, zodat betrokkene voldoende informatie heeft om een goed besluit te kunnen nemen;
- ondubbelzinnig is , waardoor geen twijfel bestaat dat betrokkene toestemming heeft gegeven.

De bewijslast dat toestemming is gegeven ligt bij VITO. Daarom zorgt VITO er voor dat toestemming alleen gegeven kan worden door een ondubbelzinnige wilsuiting of ondubbelzinnige actieve handeling van betrokkene.

Bij het vragen van toestemming informeert VITO gelijktijdig over de mogelijkheid dat de toestemming altijd weer kan worden ingetrokken.

Voor de bijzondere situatie van toestemming heeft VITO een richtlijn 'Toestemming' opgesteld (in opmaak).

4.2 Bijzondere- en strafrechtelijke persoonsgegevens

Verwerking van bijzondere- en strafrechtelijke persoonsgegevens (bijv. gegevens over ras, politieke opvattingen, religieuze overtuigingen, seksueel leven, vakbondslidmaatschap of genetische, biometrische of gezondheidsgegevens) is omwille van de gevoeligheid ervan in beginsel verboden.

VITO verwerkt bijzondere en strafrechtelijke persoonsgegevens alleen in situaties dat de privacy wet- en regelgeving hierop uitzonderingen toestaat én de verwerking gerechtvaardigd is.

De voor VITO relevante algemene uitzonderingsgronden zijn:

- de betrokkene heeft zijn uitdrukkelijke toestemming gegeven;
- de verwerking is noodzakelijk in het kader van de uitvoering van regels op het gebied van arbeids- en sociaal zekerheidsrecht;
- de verwerking heeft betrekking op persoonsgegeven die kennelijk door de betrokkene openbaar zijn gemaakt;

Daarnaast zijn er nog specifieke uitzonderingsgronden, waarin VITO bijzondere persoonsgegevens verwerkt:

- de persoonsgegevens over ras en etnische afkomst mogen verwerkt worden als dit noodzakelijk is voor de identificatie van de betrokkene;
- de biometrische gegevens mogen verwerkt worden als dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden;
- de gezondheidsgegevens mogen verwerkt worden als dit noodzakelijk is voor:
  - een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene;
  - de re-integratie of begeleiding van medewerkers of uitkeringsgerechtigden in verband met hun gezondheid;
  - de beoordeling van het door een verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt, of
  - de uitvoering van een verzekeringsovereenkomst.

Voor de specifieke betekenis van het verwerken van bijzondere persoonsgegevens heeft VITO een richtlijn 'Bijzondere Persoonsgegevens' opgesteld (in opmaak).

5. Privacy by design and by default

VITO houdt bij het ontwikkelen en opzetten van diensten en het ontwerp van nieuwe gegevenssystemen rekening met de eisen die de privacy wet- en regelgeving stellen aan bescherming van persoonsgegevens.

VITO zorgt er standaard voor dat de inbreuk op de privacy of persoonlijke levenssfeer bij de gegevensverwerking tot een minimum beperkt blijft door de toegang tot persoonsgegevens binnen de organisatie af te schermen en gebruik te maken van pseudonimisering en versleuteling van persoonsgegevens.

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert VITO voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling uit.

Met deze gegevensbeschermingseffectbeoordeling, ook wel genoemd Privacy Impact Assessment (PIA) of Data Protection Impact Assessment (DPIA), beoordeelt VITO de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens.

De gegevensbeschermingseffectbeoordeling bevat:

- een beschrijving van de beoogde verwerking en de verwerkingsdoeleinden;
- een beoordeling van de noodzakelijkheid en evenredigheid van de verwerking met betrekking tot de verwerkingsdoeleinden;
- een beoordeling van de risico's voor betrokkenen;
- de beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.

Bij het uitvoeren van een gegevensbeschermingseffectbeoordeling wordt advies ingewonnen bij de DPO.

De ontwerp- en standaardinstellingen voor een privacy by design and by default worden verder toegelicht in de richtlijn 'Privacy by design and by default' (in opmaak).

6. Bewaartermijn van persoonsgegevens

In uitvoering van artikel 5 van de GDPR en conform het verwerkingsbeginsel op opslagbeperking, worden persoonsgegevens niet langer bewaard dan noodzakelijk is voor de verwerking of het proces waarin deze gegevens worden verwerkt.

Bij het opstellen en implementeren van VITO's beleid inzake dataretentie werden drie fase onderscheiden:

- onderzoek naar eventueel van toepassing zijnde wettelijke minimum- en maximumbewaartermijnen;
- kiezen van de juiste bewaartermijnen en deze vastleggen met onderbouwing;
- implementeren van de gekozen bewaartermijnen in de toepasselijke processen en systemen.

Voor het waarborgen dat gegevens onnodig worden bijgehouden heeft VITO een 'richtlijn dataretentie' opgesteld en wordt de bewaartermijn van de persoonsgegevens opgenomen in het verwerkingsregister (in opmaak).

Hoofdstuk III - Plichten verwerkingsverantwoordelijke en verwerker

In hoofdstuk II is uiteengezet welke onderscheiden rollen en functies VITO heeft vanuit zijn bedrijfsvoering en dienstverlening en welke ertoe leiden dat VITO gegevensverwerkingen de ene keer als verwerkingsverantwoordelijke en de andere keer als verwerker is te kwalificeren. De privacy wet- en regelgeving legt zowel aan de verwerkingsverantwoordelijke alsook aan de verwerker verplichtingen op.

1. Verantwoordingsplicht

Als *verwerkingsverantwoordelijke* is VITO verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de verwerkingsbeginselen. Dat betekent dat VITO:

- de verplichtingen uit de privacy wet- en regelgeving moet naleven; en
- deze naleving moet kunnen aantonen ('accountability').

Als *verwerker* is VITO verantwoordelijk dat de gegevensverwerkingen aan hem zijn uitbesteed, op een zodanige rechtmatige en zorgvuldige wijze uitvoert dat zijn opdrachtgevers de op hun als verwerkingsverantwoordelijken rustende verantwoordingsplicht kunnen nakomen.

De wijze waarop en de maatregelen waarmee VITO deze verantwoordingsplicht invult, wordt hierna beschreven.

2. Register van verwerkingsactiviteiten

VITO houdt een centraal elektronisch register van verwerkingsactiviteiten bij.

Als *verwerkingsverantwoordelijke* noteert VITO de volgende gegevens in het register:

- naam en contactgegevens van de verwerkingsverantwoordelijke en van de DPO;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien van toepassing, doorgifte aan een land buiten de Europese Unie of een internationale organisatie;
- de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens worden gewist;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Als *verwerker* noteert VITO de volgende gegevens in het register:

- naam en contactgegevens van de verwerker, iedere verwerkingsverantwoordelijke waarvoor wordt

gehandeld, en van de DPO;
- de categorieën van verwerkingen die voor iedere verwerkingsverantwoordelijke zijn uitgevoerd;
- indien van toepassing, doorgifte aan een land buiten de Europese Unie of een internationale organisatie;
- een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.

3. Verwerkersovereenkomst

Als VITO als verwerkingsverantwoordelijke een verwerker inschakelt voor zijn gegevensverwerkingen, sluit hij met deze een schriftelijke, waaronder elektronische, overeenkomst waarin de volgende zaken worden geregeld:
- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van VITO.

In de verwerkersovereenkomst wordt ten aanzien van de verwerker vastgelegd dat deze:
- de persoonsgegevens alleen verwerkt onder schriftelijke instructies van VITO;
- waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde en aan geheimhouding gebonden personen;
- een passend beveiligingsniveau hanteert;
- VITO alle mogelijke ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
- VITO bijstaat bij het nakomen van zijn verplichtingen op het gebied van beveiliging van persoonsgegevens, de meldplicht datalekken en het uitvoeren van een privacy impact assessment;
- na beëindiging van de overeenkomst de verwerkte persoonsgegevens wist of aan VITO teruggeeft, en bestaande kopieën verwijdert;
- VITO alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de privacy wet en regelgeving rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- geen subverwerkers in dienst neemt zonder voorafgaande schriftelijke toestemming van VITO en met deze subverwerkers eenzelfde (sub)verwerkersovereenkomst afsluit als hijzelf met VITO heeft afgesloten.

Als VITO als verwerker in opdracht van opdrachtgevers gegevensverwerkingen verricht, is de opdrachtgever verantwoordelijke voor het afsluiten van de verwerkersovereenkomst. VITO is op grond van die overeenkomst verplicht de daarin opgenomen verplichtingen na te komen.

Hoofdstuk IV - Persoonsgegevensbeveiliging

In dit hoofdstuk wordt stilgestaan bij de verplichting om met betrekking tot de gegevensverwerkingen een passend beveiligingsniveau te waarborgen.

1. Passende beveiliging

VITO neemt passende technische en organisatorische maatregelen om een op het verwerkingsrisico afgestemd passend beveiligingsniveau te waarborgen. Deze maatregelen omvatten onder meer:
- pseudonimisering en versleuteling van de persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- 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.

2. Informatiebeveiligingsbeleid

VITO heeft zijn informatiebeveiligingsbeleid vastgelegd in zijn ‘Informatiebeveiliging@VITO’.

Het beleidsdocument Informatiebeveiliging@VITO beschrijft de wijze waarop VITO informatiebeveiliging risico’s identificeert, evalueert, beheerst en bewaakt.

3. Melden datalekken

Een inbreuk in verband met persoonsgegevens ('datalek') is een inbreuk op de beveiliging van persoonsgegevens die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Voor de situatie dat zich een datalek voordoet, heeft VITO een procedure melden datalekken ingericht dat verloopt via de VITO Incidentenregeling of, ingeval van bijzondere datalekken ('foutieve correspondentie'), middels specifiek daarvoor ingerichte procedures.

Deze procedure omvat onder meer:

- een intern meldadres meldendatalekken@VITO.nl waarop datalekken kunnen worden gemeld bij de functionaris gegevensbescherming;
- een meldingsformulier datalekken;
- een handleiding melden datalekken.

Als VITO als verwerkingsverantwoordelijke kwalificeert en voor zijn gegevensverwerking een beroep doet op een verwerker, maakt VITO met deze verwerker middels den verwerkersovereenkomst de afspraak dat de verwerker een bij zijn gegevensverwerking geconstateerd datalek zo snel als mogelijk meldt bij VITO.

Als VITO als verwerker kwalificeert, draagt VITO er zorg voor dat wanneer bij zijn in opdracht verrichte gegevensverwerkingen een datalek plaatsvindt, dit zo snel als mogelijk wordt gemeld bij de opdrachtgever.

4. Melden bij de toezichthouder

Een datalek meldt VITO uiterlijk binnen 72 uur bij de Vlaamse Toezichtscommissie tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de betrokkenen.

Bij de melding aan de Vlaamse Toezichtscommissie wordt ten minste het volgende omschreven of meegedeeld:

- de aard van het datalek;
- waar mogelijk de categorieën van betrokkenen en, bij benadering, het aantal betrokkenen;
- de naam en de contactgegevens van de DPO of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek; en
- de maatregelen die VITO voorgesteld of genomen heeft om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De melding aan de Vlaamse Toezichtscommissie wordt gedaan door de DPO.

VITO houdt een overzicht bij van de aan de Vlaamse Toezichtscommissie gemelde datalekken.

5. Melden bij de betrokkene

Wanneer het datalek waarschijnlijk een hoog risico voor betrokkenen inhoudt, meldt VITO het datalek zo snel als mogelijk ook aan betrokkenen.

Mededeling aan betrokkenen kan achterwege blijven wanneer:

- VITO passende technische en organisatorische beschermingsmaatregelen heeft genomen, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- VITO achteraf maatregelen heeft genomen waarmee de vastgestelde risico's voor betrokkenen zich waarschijnlijk niet meer zullen voordoen;
- de melding aan betrokkenen VITO onevenredig veel inspanning zou kosten. In dat geval kan de informatie over het datalek op de website van VITO worden gepubliceerd.

Bij de melding aan betrokkenen wordt ten minste het volgende omschreven of meegedeeld:

- de aard van het datalek;
- de naam en de contactgegevens van de functionaris gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek; en
- de maatregelen die VITO voorgesteld of genomen heeft om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Hoofdstuk V – Datatransfers

In dit hoofdstuk wordt aangegeven hoe VITO omgaat indien en voor zover er bij gegevensverwerkingen persoonsgegevens worden doorgegeven aan andere partijen.

1. Binnen de Europese Unie

Landen binnen de Europese Unie bieden eenzelfde beschermingsniveau als België. Bij datatransfers naar entiteiten of personen die gevestigd zijn binnen de Europese Unie, worden door VITO steeds de algemene principes van de GDPR gevolgd, zoals rechtsmatigheid, transparantie en overeenstemming met het oorspronkelijk doel.

2. Buiten de Europese Unie

VITO mag alleen persoonsgegevens aan entiteit of persoon, die gevestigd zijn in een land buiten de Europese Unie, doorgegeven als daarmee het door de GDPR vereiste beschermingsniveau niet wordt ondermijnd. Er zijn vier gevallen waarbij zulke datatransfers mogelijk zijn, die als volgt in detail worden besproken.

1.1 Adequaatheidsbesluiten

Landen die een met de GDPR vergelijkbaar niveau van gegevensbescherming bieden in hun nationale wetgeving worden geacht een passend niveau van gegevensbescherming te bieden. De Europese Commissie stelt vast of dit het geval is en neemt dan een 'adequaatheidsbesluit'.

Alle landen met een adequaatheidsbeslissing zijn te vinden op de website van de Europese Commissie:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents

1.2 Passende waarborgen

Doorgifte van persoonsgegevens aan een land buiten de Europese Unie of een internationale organisatie waarvoor geen adequaatheidsbesluit is afgegeven, is alleen toegestaan als dat land of die organisatie passende waarborgen bieden.

Van passende waarborgen is sprake ingeval van:

- contractuele bepalingen (modelovereenkomst Europese Commissie of andere passende contractuele bepalingen); of
- bindende bedrijfsvoorschriften laten bedrijven, die in meerdere landen actief zijn, toe om tussen verschillende vestigingen van het bedrijf (buiten de Europese Unie) gegevens door te geven, door middel van bindende waarborgen.

1.3 Afwijkingen

Als er geen adequaatheidsbesluiten of passende waarborgen zijn, zal VITO als afwijking hiervan alleen persoonsgegevens doorgeven wanneer:

- betrokkene uitdrukkelijk toestemming heeft gegeven;
- dit noodzakelijk is voor de uitvoering van precontractuele maatregelen of van een overeenkomst tussen betrokkene en VITO;
- dit noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen VITO en een derde gesloten overeenkomst; dit noodzakelijk is ten behoeve van een rechtsvordering;
- dit noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven; of
- dit is verricht vanuit een register dat volgens het Unierecht of het nationaal recht van een lidstaat is bedoeld om het publiek voor te lichten.

1.4 Uitzonderingen

Als er geen adequaatheidsbesluit of passende waarborgen zijn en geen afwijkingen van toepassing zijn, zal VITO als uitzondering hierop alleen persoonsgegevens doorgeven wanneer de doorgifte:

- niet repetitief is;
- een beperkt aantal betrokkenen betreft;
- noodzakelijk is voor dwingende gerechtvaardigde belangen van VITO die niet ondergeschikt zijn aan de

belangen van de betrokkene; en
- gewaarborgd is met passende beschermingsmaatregelen door VITO.

Als doorgifte op basis van deze cumulatieve uitzonderingsgronden plaatsvindt, informeert VITO zowel de Vlaamse Toezichtscommissie als de betrokkene over de doorgifte.

VITO heeft een richtlijn 'Datatransfers' voor het doorgeven van persoonsgegevens aan een land buiten de Europese Unie opgesteld (in opmaak).

Hoofdstuk VI - Rechten betrokkene

VITO houdt in dit beleid rekening met de grondgedachte achter de GDPR dat de betrokkene een eerlijke en transparante verwerking van persoonsgegevens moet kunnen verwachten en waarbij hij deze rechten op een gemakkelijke en eenvoudige wijze moet kunnen uitoefenen tegen de verwerkingsverantwoordelijke.

1. Recht op informatie

VITO informeert de betrokkene, op een actieve wijze, over de gegevensverwerkingen en communiceert met hem over zijn rechten in duidelijke en eenvoudige taal VITO draagt er zorg voor dat deze informatie en communicatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm plaatsvindt. Dit kan schriftelijk, maar ook met elektronische middelen gebeuren. Als betrokkene daarom verzoekt, kan dit zelfs mondeling.

De VITO privacyverklaring, evenals dit gegevensbeschermingsbeleid, zijn belangrijke onderdelen in de informatieplicht van VITO. VITO gaat hierbij uit van een gelaagde aanpak van deze informatieplicht. Details van de verwerking van persoonsgegevens door VITO worden steeds opgenomen in het verwerkingsregister.

VITO faciliteert de betrokkene in de uitoefening van zijn rechten. Dit kan door het beschikbaar stellen van een digitale voorziening dan wel van een standaardformulier.

Het verstrekken van de informatie, de communicatie of het treffen van de maatregelen om de rechten te kunnen uitoefenen, gebeurt kosteloos. Alleen wanneer de verzoeken van de betrokkene kennelijk ongegrond of buitensporig zijn, kan VITO:
- een redelijke administratieve vergoeding aanrekenen; of
- de verzoeken zelfs weigeren.

2. Recht op inzage

Indien de betrokkene gebruik maakt van zijn recht om inzage te krijgen in de persoonsgegevens die VITO van hem verwerkt, verleent VITO hem deze inzage en geeft hem informatie over:
- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- de (categorieën van) ontvangers van de persoonsgegevens;
- indien mogelijk, hoe lang de persoonsgegevens worden bewaard;
- het recht op verbetering, wissen, beperking en bezwaar;
- het recht om klacht in te dienen bij de Vlaamse Toezichtscommissie;
- de bron van die gegevens als ze niet van betrokkene zelf afkomstig zijn;
- indien van toepassing, het bestaan van geautomatiseerde besluitvorming, waaronder profilering, het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer VITO de persoonsgegevens doorstuurt naar een land buiten de Europese Unie, informeert VITO de betrokkene over de passende waarborgen inzake deze doorgifte.

De genoemde informatie wordt middels een kopie verstrekt. Wanneer de betrokkene zijn verzoek elektronisch indient, verstrekt VITO de informatie in een gangbare elektronische vorm.

Indien het verzoek bijzondere persoonsgegevens betreft, kan de DPO een inzage ter plaatse voorstellen en hiervoor de plaats en datum bepalen.

3. Recht op verbetering

Indien de betrokkene gebruik maakt van zijn recht op verbetering, zorgt VITO ervoor dat de betrokkene zijn persoonsgegevens worden verbeterd indien deze onjuist of onvolledig zijn.

VITO stelt partijen met wie de persoonsgegevens die worden verbeterd of aangevuld, gedeeld zijn op de hoogte

van de wijzigingen. Dit informeren blijft achterwege wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

4. Recht op gegevenswissing

Indien de betrokkene gebruik maakt van zijn recht op gegevenswissing, zal VITO de persoonsgegevens van de betrokkene zo snel mogelijk wissen in een van de volgende situaties:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verwerkt;
- betrokkene trekt zijn toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
- betrokkene heeft gegrond bezwaar gemaakt tegen een verwerking:
  - op basis van onder meer de grondslag noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde; of
  - ten behoeve van direct marketing;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op VITO rust.

Naast het recht op wissing heeft de betrokkene onder bepaalde omstandigheden ook het recht om vergeten te worden ('vergetelheid'). Het gaat hier om de situatie waarbij de verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijv. door ze online te zetten). Het recht om vergeten te worden geldt voor iedereen, maar in het bijzonder bij de verwerking van gegevens van kinderen.

Deze situatie is feitelijk niet aan de orde voor de gegevensverwerkingen die VITO verricht. VITO plaatst niet publiekelijk, d.w.z. openbaar op internet persoonsgegevens van betrokkenen. Daarmee is het recht op vergetelheid op VITO niet van toepassing.

VITO stelt partijen met wie de persoonsgegevens die worden verbeterd, gedeeld zijn op de hoogte van de wijzigingen. Dit informeren blijft achterwege wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

5. Recht op beperking

Indien de betrokkene gebruik maakt van zijn recht op beperking van de verwerking, stopt VITO de gegevensverwerking wanneer:

- de juistheid van de persoonsgegevens worden betwist;
- de verwerking onrechtmatig is;
- VITO de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene ze nodig ten behoeve van een rechtsvordering;
- de betrokkene bezwaar maakt tegen de verwerking op basis van de rechtsgrond gerechtvaardigd belang in afwachting van de vraag of de gerechtvaardigde belangen van VITO zwaarder wegen dan die van de betrokkenen.

Wanneer de verwerking is beperkt, verwerkt VITO alleen nog persoonsgegevens:

- met toestemming van de betrokkene;
- in het kader van een rechtsvordering; of
- ter bescherming van de rechten van andere personen.

VITO stelt partijen met wie de persoonsgegevens die worden beperkt, gedeeld zijn op de hoogte van de beperkingen. Dit informeren blijft achterwege wanneer:

- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

6. Recht op bezwaar

Indien de betrokkene gebruik maakt van zijn recht op bezwaar tegen gegevensverwerking op basis van de grondslag gerechtvaardigd belang, stopt VITO de verwerking, tenzij de belangen voor VITO om de

persoonsgegevens te verwerken zwaarder wegen dan de belangen van de betrokkene om de gegevensverwerking te staken.

Indien de betrokkene bezwaar maakt tegen de verwerking van persoonsgegevens voor direct marketing, stopt VITO de verwerking onmiddellijk en onvoorwaardelijk.

VITO informeert de betrokkene over dit recht bij het eerste contact bij gegevensverwerking op basis van gerechtvaardigd belang en bij het eerste direct marketing-contact.

7. Recht op gegevensoverdraagbaarheid

Indien de betrokkene gebruik maakt van zijn recht op overdraagbaarheid van de persoonsgegevens die hijzelf aan VITO heeft verstrekt ('dataportabiliteit'), zorgt VITO ervoor dat de betrokkene een kopie krijgt van deze gegevens krijgt in een gestructureerde, gangbare en machineleesbare vorm.

Het recht op overdraagbaarheid geldt alleen voor de door de betrokkene verstrekte gegevens die geautomatiseerd (digitaal) worden verwerkt op basis van de grondslagen:

- ondubbelzinnige dan wel uitdrukkelijke toestemming van de betrokkene;
- noodzakelijk voor de uitoefening van de overeenkomst met de betrokkene.

8. Recht om niet aan geautomatiseerde besluitvorming onderworpen te worden

De betrokkene heeft het recht om niet te worden onderworpen aan een enkel op geautomatiseerde verwerking (waaronder profilering) gebaseerd besluit, wanneer dit:

- rechtsgevolgen heeft voor hem; of
- het hem anderszins in aanzienlijke mate treft.

VITO staakt een dergelijke verwerking, tenzij:

- dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;
- dit is toegestaan bij wet.

Indien gebruik wordt gemaakt van de eerste twee uitzonderingen, neemt VITO maatregelen die tenminste het volgende omvatten:

- het recht op menselijke tussenkomst;
- het recht voor de betrokkene om zijn standpunt kenbaar te maken; en
- het recht om het besluit aan te vechten.

Betrokken kunnen steeds een verzoek indienen bij VITO, voor het uitoefenen van hun rechten.

VITO informeert de betrokkene, uiterlijk binnen een maand na ontvangst van het verzoek, om uitvoering van zijn rechten over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek kan deze termijn met nog eens met twee maanden worden verlengd. Van deze verlenging wordt de betrokkene binnen een maand na ontvangst van het verzoek in kennis gesteld.

Wanneer VITO geen gevolg geeft aan het verzoek, wordt dit aan de betrokkene, uiterlijk binnen een maand na ontvangst van het verzoek, gemotiveerd meegedeeld. Ook informeert VITO hem daarbij op de mogelijkheid om klacht in te dienen bij de Vlaamse Toezichtscommissie of Gegevensbeschermingsautoriteit en beroep bij de rechter.

Hoofdstuk VII – Klacht en beroep

Iedere betrokkene heeft het recht om een klacht in te dienen indien hij van mening is dat de verwerking van hem betreffende persoonsgegevens door VITO een inbreuk maakt op de GDPR.

De klachtenprocedure bij de Vlaamse Toezichtscommissie kan je terugvinden op de volgende link: https://overheid.vlaanderen.be/klachtenprocedure-vtc. Een onderdeel van de procedure is het invullen van een klachtenformulier, terug te vinden op bovenvermelde link.

De klachtenprocedure bij de Gegevensbeschermingsautoriteit kan je terugvinden op volgende link: https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen. Een onderdeel van de procedure is het invullen van een klachtenformulier, terug te vinden op bovenvermelde link.