VERWERKERSOVEREENKOMST

MAGDA DOCUMENTENDIENST

tussen

STAD LIER

en

DIGITAAL VLAANDEREN

DEZE VERWERKERSOVEREENKOMST WORDT AANGEGAAN TUSSEN:

Stad Lier, ingeschreven in het KBO met nummer 0207.502.301. met zetel Paradeplein 2 bus 1, 2500 Lier, vertegenwoordigd door het college van burgemeester en schepenen, voor wie tekenen: Rik Verwaest (burgemeester) en Katrijn Bosschaerts (algemeen directeur).

Bovengenoemde partij wordt ook aangeduid als de "**opdrachtgevende instantie**"

EN

HET VLAAMS GEWEST, vertegenwoordigd door de Vlaamse Regering, bij delegatie, in de persoon van de leidend ambtenaar van het intern verzelfstandigd agentschap zonder rechtspersoonlijkheid agentschap Digitaal Vlaanderen, administrateur-generaal Jan Smedts, gevestigd te Havenlaan 88, 1000 Brussel, ingeschreven in het KBO met nummer 0316.380.841 (hierna "**Digitaal Vlaanderen**")

Bovengenoemde partij wordt ook aangeduid als de **"verwerker"**.

De opdrachtgevende instantie en Digitaal Vlaanderen worden gezamenlijk ook aangeduid als de "**partijen**" of afzonderlijk als de "**partij**".

OVERWEGENDE DAT

A. Digitaal Vlaanderen is een intern verzelfstandigd agentschap van de Vlaamse overheid met onder meer de taak om instanties te ondersteunen in hun contacten met burgers, ondernemingen en organisaties en hun digitalisering en vereenvoudiging van dienstverlening en processen , dit overeenkomstig artikels 4,6° en 4,8° van het besluit van de Vlaamse regering van 18 maart 2016 houdende de oprichting van het intern verzelfstandigd agentschap Digitaal Vlaanderen, de bepaling van diverse maatregelen voor de ontbinding zonder vereffening van het AGIV, de regeling van de overdracht van de activiteiten en het vermogen van het AGIV aan het agentschap Digitaal Vlaanderen en de vaststelling van de werking, het beheer en de boekhouding van het Eigen Vermogen Digitaal Vlaanderen. In dat kader biedt Digitaal Vlaanderen een dienstverlening aan waarbij ze de aansluiting voorziet met het door de opdrachtgevende instantie (de entiteit die digitaal documenten wenst te versturen) gewenste kanaal, zijnde hetzij een beveiligde elektronische brievenbus (de eBox voor natuurlijke personen en/of de eBox voor ondernemingen), hetzij een print- en leverdienstenleverancier om digitale documenten via een analoge postdienst te verzenden. Daarnaast biedt Digitaal Vlaanderen een dienstverlening aan waarbij ze als document provider eBox-documenten gedurende een door de opdrachtgevende instantie bepaalde termijn voor ontsluiting ter beschikking stelt aan de HIP's.

B. De opdrachtgevende instantie wenst beroep te doen op de dienstverlening van Digitaal Vlaanderen zoals omschreven onder A.

C. In het kader van deze dienstverlening zal Digitaal Vlaanderen bepaalde persoonsgegevens verwerken ten behoeve van de opdrachtgevende instantie. De partijen wensen nu hun afspraken met betrekking tot de uitvoering en organisatie van deze verwerking van persoonsgegevens te formaliseren in deze verwerkersovereenkomst.

WERD HET VOLGENDE OVEREENGEKOMEN:

1. Definities

- Aanbieder van eBox: eBox bestaat enerzijds uit eBox burger, een dienst aangeboden door de FOD Beleid en Ondersteuning en anderzijds uit eBox ondernemingen, een dienst aangeboden door de Rijksdienst voor Sociale Zekerheid;
- Bestemmeling: de natuurlijke persoon of rechtspersoon, of een vertegenwoordiger hiervan, voor wie de eBox-documenten bestemd zijn;
- Document provider: de dienstenintegrator of het technisch platform toebehorende aan een overheidsinstantie die de eBox-documenten ter beschikking stelt van de bestemmeling zodat deze door de HIP kunnen worden ontsloten
- eBox: de dienst die overheidsinstanties toelaat om elektronische berichten uit te wisselen met natuurlijke personen (eBox burger) of ondernemingen en hun vertegenwoordigers (eBox ondernemingen).
- eBox-documenten: de documenten die door een overheidsinstantie via de eBox naar een bestemmeling worden verzonden;
- HIP: de dienstverlener die op vraag van de bestemmeling de documenten die door de document provider in de eBox worden bewaard, ontsluit;

2. Verwerkingsopdracht

Digitaal Vlaanderen verwerkt de persoonsgegevens uitsluitend overeenkomstig de verwerkingsopdracht, de in deze verwerkersovereenkomst vastgelegde verplichtingen en de toepasselijke wetgeving. Digitaal Vlaanderen verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van de opdrachtgevende instantie. Digitaal Vlaanderen beschouwt de verwerkingsopdracht als de volledige instructie van de opdrachtgevende instantie.

De verwerkingsopdracht wordt nader omschreven in bijlage 1 bij deze overeenkomst.

3. Naleving van de wetgeving

Digitaal Vlaanderen verbindt zich ertoe om de wet- en regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens na te leven.

De opdrachtgevende instantie verbindt er zich toe de wet- en regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens na te leven.

Indien Digitaal Vlaanderen van oordeel is dat de verwerkingsopdracht niet of niet meer in overeenstemming is met de relevante wet- of regelgeving, licht ze de opdrachtgevende instantie daarover in en kan ze de verwerking tijdelijk of permanent stopzetten.

4. Contact

Elke partij duidt een contactpunt aan voor de aangelegenheden met betrekking tot de verwerking van persoonsgegevens in het kader van deze verwerkersovereenkomst (hierna: de "SPOC"). De contactgegevens van de verschillende SPOC's worden doorgegeven via het aanvraagformulier voor de diensten. Wanneer een SPOC gedurende de looptijd van deze verwerkersovereenkomst zou wijzigen, moet dit gemeld worden aan de partijen, zonder dat evenwel een aanpassing van deze overeenkomst noodzakelijk is.

5. Doorgifte

Digitaal Vlaanderen zal de persoonsgegevens die verwerkt worden niet doorgeven aan enige derde partij anders dan noodzakelijk voor de uitvoering van de verwerkingsopdracht, tenzij dit noodzakelijk is om te voldoen aan een Vlaamse, federale of Europese verplichting. In dat geval zal Digitaal Vlaanderen de opdrachtgevende instantie voorafgaandelijk aan de doorgifte in kennis stellen van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

6. Vertrouwelijkheid personeel

Alle medewerkers van Digitaal Vlaanderen, zowel intern als extern, gemachtigd tot het uitvoeren van de verwerkingsopdracht, zijn gehouden tot een wettelijke dan wel contractuele vertrouwelijkheidsverplichting.

7. Onderverwerking

De opdrachtgevende instantie gaat akkoord met het gebruik van de onderverwerker(s) zoals vermeld in bijlage 2.

Digitaal Vlaanderen kan onderverwerkers toevoegen of vervangen. Desgevallend waarborgt Digitaal Vlaanderen dat deze nieuwe onderverwerkers voldoende garanties bieden opdat de verwerking aan de vereisten van de verordening 2016/679 van het Europees parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna de 'algemene verordening gegevensbescherming') voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. De opdrachtgevende instantie krijgt ten minste dertig dagen voor een wijziging van de onderverwerker een notificatie.

De opdrachtgevende instantie kan gedurende deze dertig dagen gemotiveerd bezwaar aantekenen tegen een aanstelling van een nieuwe onderverwerker. In dat geval zullen Digitaal Vlaanderen en de opdrachtgevende instantie gezamenlijk tot een oplossing proberen komen en zal derhalve overeengekomen worden dat:

- de onderverwerker alsnog zal worden ingeschakeld; of
- de onderverwerker zal worden vervangen door een andere door Digitaal Vlaanderen voorgestelde onderverwerker; of
- de onderverwerker die Digitaal Vlaanderen heeft voorgesteld, niet zal worden aangesteld.

Bij gebrek aan enig akkoord heeft de opdrachtgevende instantie het recht om de verwerkingsopdracht kosteloos te beëindigen.

Indien Digitaal Vlaanderen beroep doet op een onderverwerker, is het volgende altijd van toepassing:

- de aanstelling van een onderverwerker doet geen afbreuk aan de verplichtingen die op Digitaal Vlaanderen rusten overeenkomstig de verwerkingsopdracht of deze verwerkersovereenkomst;
- Digitaal Vlaanderen zal met haar aangestelde onderverwerkers een overeenkomst afsluiten waarin minstens de verplichtingen inzake gegevensbescherming van deze verwerkersovereenkomst zijn opgenomen; en
- Digitaal Vlaanderen blijft ten aanzien van de opdrachtgevende instantie volledig verantwoordelijk voor de verplichtingen waarvoor zij beroep doet op een onderverwerker.

8. Technische en organisatorische maatregelen

Digitaal Vlaanderen treft alle passende technische en organisatorische maatregelen om het beveiligingsniveau van de verwerking te waarborgen, hierbij rekening houdende met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

De technische en organisatorische maatregelen die door Digitaal Vlaanderen worden getroffen worden als bijlage 3 aan deze verwerkersovereenkomst gehecht. Indien Digitaal Vlaanderen zou oordelen dat bijkomende technische en organisatorische maatregelen dienen te worden getroffen, licht ze de opdrachtgevende instantie hierover in.

9. Rechten betrokkene

Digitaal Vlaanderen staat de opdrachtgevende instantie bij in haar verplichting te antwoorden op verzoeken van een betrokkene tot uitoefening van zijn rechten zoals vastgesteld in de toepasselijke wet- en regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens. Dit houdt in dat Digitaal Vlaanderen de betrokken opdrachtgevende instantie zo snel mogelijk op de hoogte zal stellen indien zij dergelijk verzoek ontvangt en op vraag van de betrokken opdrachtgevende instantie de nodige verwerkingshandelingen zal stellen die volgen uit de uitoefening van deze rechten.

10. Inbreuken

In geval van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (hierna: de 'inbreuk in verband met persoonsgegevens') brengt Digitaal Vlaanderen de opdrachtgevende instantie daarvan zonder onredelijke vertraging op de hoogte.

De melding omvat, voor zover deze informatie voor Digitaal Vlaanderen beschikbaar is:

- de aard van de inbreuk in verband met persoonsgegevens, indien mogelijk met vermelding van de categorieën van betrokkenen en, bij benadering, het aantal betrokkenen;

- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

- de maatregelen die Digitaal Vlaanderen voorstelt te nemen en/of reeds heeft genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan;

- de naam en de contactgegevens van de functionaris voor gegevensbescherming van Digitaal Vlaanderen.

De melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en eventueel aan de betrokkene blijft uitsluitend de verantwoordelijkheid van de opdrachtgevende instantie. Digitaal Vlaanderen zal hier wel indien gevraagd de nodige bijstand bij verlenen.

11. Audits

Digitaal Vlaanderen zal op vraag van de opdrachtgevende instantie alle informatie ter beschikking stellen die redelijkerwijs is vereist in het kader van een audit of inspectie door de opdrachtgevende instantie of een door de opdrachtgevende instantie gemachtigde controleur. Elke audit die door een opdrachtgevende instantie gevraagd of uitgevoerd wordt, zal volledig op kosten van deze opdrachtgevende instantie gebeuren.

12. Internationale doorgifte van de gegevens

Digitaal Vlaanderen zal de persoonsgegevens niet doorgeven of bewaren buiten de landen van de Europese Economische Ruimte (EER), tenzij dit uitdrukkelijk in de verwerkingsopdracht gevraagd wordt of wanneer dit noodzakelijk zou zijn om te voldoen aan een wettelijke verplichting of een gerechtelijk bevel.

13. Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging

Digitaal Vlaanderen zal – rekening houdende met de aard van de verwerking en de ter haar beschikking staande informatie – de opdrachtgevende instantie desgevallend bijstaan in haar verplichting tot het opstellen van een gegevensbeschermingseffectbeoordeling, inzonderheid om te komen tot een volwaardige en correcte risicobeoordeling en -beheersing. Dit met name door een overzicht te geven van de technische en organisatorische maatregelen die getroffen werden. In het bijzonder zal de opdrachtnemer alle maatregelen die genomen zijn in het kader van informatieveiligheid ter beschikking stellen aan de opdrachtgever. Desgevallend zal Digitaal Vlaanderen eveneens haar bijstand verlenen bij een voorafgaande raadpleging aan de toezichthoudende autoriteit.

14. Inwerkingtreding, duur en beëindiging

Deze verwerkersovereenkomst treedt in werking op datum van ondertekening en is van onbepaalde duur. Ze eindigt van rechtswege na beëindiging van de verwerkingsopdracht.

Na beëindiging van de verwerkingsopdracht zal Digitaal Vlaanderen, naar keuze van de opdrachtgevende instantie, alle persoonsgegevens met betrekking tot de verwerkingsopdracht verwijderen of terugbezorgen en bestaande kopieën verwijderen. Digitaal Vlaanderen kan kopieën bewaren indien de opslag van persoonsgegevens verplicht is ingevolge een wettelijke verplichting.

15. Aansprakelijkheid

Digitaal Vlaanderen kan alleen aansprakelijk worden gesteld voor de bewezen schade die door een toerekenbare fout van Digitaal Vlaanderen of een onderverwerker van Digitaal Vlaanderen werd veroorzaakt ingevolge het bij de verwerking niet voldoen aan de specifiek tot verwerkers gerichte verplichtingen van de AVG, deze verwerkingsovereenkomst of ingevolge het buiten dan wel in strijd met de rechtmatige instructies van de opdrachtgevende instantie handelen.

16. Diversen

Indien een bepaling van deze verwerkingsovereenkomst geheel of gedeeltelijk ongeldig of niet-afdwingbaar wordt geacht, wordt deze (voor zover deze ongeldig of niet-afdwingbaar is) als scheidbaar beschouwd en wordt de geldigheid van de andere bepalingen van deze verwerkingsovereenkomst niet aangetast.

Aanvullingen en wijzigingen op deze verwerkersovereenkomst dienen schriftelijk te gebeuren door middel van een addendum dat als bijlage aan deze verwerkersovereenkomst zal worden gehecht.

Deze overeenkomst omvat alle afspraken met betrekking tot de MAGDA Documentendienst en vervangt alle overeenkomsten hieromtrent die deze overeenkomst predateren.

Deze overeenkomst werd elektronisch opgesteld en ondertekend.

Voor Digitaal Vlaanderen

_____

Jan Smedts

Administrateur-generaal

Digitaal Vlaanderen

Voor de opdrachtgevende instantie

_____

Katrijn Bosschaerts	Rik Verwaest
Algemeen directeur	Burgemeester
Stad Lier	Stad Lier

Bijlagen:

- Bijlage 1: verwerkingsopdracht
- Bijlage 2: onderverwerkers
- Bijlage 3: technische en organisatorische maatregelen

BIJLAGE 1: VERWERKINGSOPDRACHT

De verwerkingsopdracht bestaat uit één of meerdere van onderstaande dienst(en):

1. Aansluiting eBox voor natuurlijke personen.

Doel van de verwerking:

Om de authenticiteit en integriteit van de berichten te waarborgen worden metadata over het document en metadata over iedere individuele transactie bijgehouden.

Soort persoonsgegevens:

Digitaal Vlaanderen verwerkt onderstaande persoonsgegevens in het kader van de aansluiting op de eBox voor natuurlijke personen:

a. het INSZ-nummer van de bestemmeling;
b. alle informatie vervat in het document dat de opdrachtgevende instantie via de eBox voor natuurlijke personen wenst te versturen.

Duur van de verwerking:

In het kader van deze dienst wordt het document zelf door Digitaal Vlaanderen bewaard in onze rol van document provider (zie punt 4), gedurende een door de opdrachtgevende instantie bepaalde periode.

Metadata over het document en metadata over iedere individuele transactie (met inbegrip van de unieke identificator van de bestemmeling) worden gedurende 10 jaar bewaard in een logdatabank.

Categorieën van betrokkenen:

Het betreft de burgers naar wie de opdrachtgevende instantie een document wenst te sturen via de eBox voor natuurlijke personen.

2. Aansluiting eBox voor ondernemingen

Doel van de verwerking:

Om de authenticiteit en integriteit van de berichten te waarborgen worden metadata over het document en metadata over iedere individuele transactie bijgehouden.

Soort persoonsgegevens:

Digitaal Vlaanderen verwerkt onderstaande persoonsgegevens in het kader van de aansluiting op de eBox voor ondernemingen:

a. de naam van ondernemingen waarbij een natuurlijke persoon kan worden geïdentificeerd.
b. alle informatie vervat in het document dat de opdrachtgevende instantie via de eBox voor ondernemingen wenst te versturen

Duur van de verwerking:

In het kader van deze dienst wordt het document zelf door Digitaal Vlaanderen bewaard in onze rol van document provider (zie punt 4), gedurende een door de opdrachtgevende instantie bepaalde periode.

Metadata over het document en metadata over iedere individuele transactie (met inbegrip van de unieke identificator van de bestemmeling) worden gedurende 10 jaar bewaard in een logdatabank.

Categorieën van betrokkenen:

Het betreft de ondernemingen waarnaar de opdrachtgevende instantie een document wenst te sturen via de eBox voor ondernemingen.

3. Aansluiting print- en leverdienstenleverancier

Doel van de verwerking:

Digitaal Vlaanderen zorgt voor de technische integratie met de print- en leverdienstenleverancier. Daarnaast houdt Digitaal Vlaanderen de authentieke digitale documenten gedurende de door de opdrachtgevende instantie bepaalde termijn in een beveiligde omgeving bij zodat deze binnen deze termijn door de bestemmeling kunnen worden opgevraagd. Om de authenticiteit en integriteit van de berichten te waarborgen worden metadata over het document en metadata over iedere individuele transactie bijgehouden.

Soort persoonsgegevens:

Digitaal Vlaanderen verwerkt onderstaande persoonsgegevens in het kader van deze dienstverlening:

a. de naam en het adres van de bestemmeling;
b. alle informatie vervat in het document dat de opdrachtgevende instantie via de print- en leverdienstenleverancier wenst te sturen.

Duur van de verwerking:

De authentieke digitale documenten worden gedurende de door de opdrachtgevende instantie bepaalde termijn bewaard zodat deze door de bestemmeling kunnen worden opgevraagd.

Metadata over het document en metadata over iedere individuele transactie (met inbegrip van de unieke identificator van de bestemmeling) worden gedurende 10 jaar bewaard in een logdatabank.

Categorieën van betrokkenen:

Het betreft zowel de burgers naar wie de opdrachtgevende instantie een document wenst te sturen als ondernemingen waarnaar de opdrachtgevende instantie een document wenst te sturen.

4. Digitaal Vlaanderen als document provider

Doel van de verwerking

Digitaal Vlaanderen zal als document provider de e-Box-documenten die de opdrachtgevende instantie via de eBox wenst te verzenden, ter beschikking stellen aan de bestemmeling. Hiertoe zal Digitaal Vlaanderen:

- De eBox-documenten gedurende een door de opdrachtgevende instantie bepaalde periode bewaren;
- Een kennisgeving van de ontvangst van de eBox-documenten bezorgen aan de HIP's;
- Een kennisgeving bezorgen aan de opdrachtgevende instantie wanneer de eBox-documenten werden geraadpleegd, indien deze wordt gebruikt door de opdrachtgevende instantie;
- Een kennisgeving bezorgen aan de opdrachtgevende instantie indien de bestemmeling geen toestemming heeft gegeven om de eBox-documenten via de eBox worden verzonden, dan wel indien deze toestemming werd ingetrokken;
- In overeenstemming met de richtlijnen van de aanbieder van de eBox de nodige logdata inzamelen, bewaren en delen.

Soort persoonsgegevens

Digitaal Vlaanderen verwerkt naast alle persoonsgegevens die in het kader van bovenstaande dienst(en) verwerkt worden ook:

- de eBox-documenten.

Duur van de verwerking

De eBox-documenten worden door Digitaal Vlaanderen bewaard gedurende een door de opdrachtgevende instantie bepaalde periode.

Metadata over het document en metadata over iedere individuele transactie (met inbegrip van de unieke identificator van de bestemmeling) worden gedurende 10 jaar bewaard in een logdatabank.

Categorieën van betrokkenen

Het betreft zowel de burgers naar wie de opdrachtgevende instantie een document wenst te sturen via de eBox voor natuurlijke personen, als de ondernemingen waarnaar de opdrachtgevende instantie een document wenst te sturen via de eBox voor ondernemingen.

5. <u>Bezorgen van de documenten via MAGDA Online</u>

Doel van de verwerking

De opdrachtgevende instantie bezorgt de documenten in het kader van de hierboven omschreven dienstverlening(en) aan Digitaal Vlaanderen via de webapplicatie MAGDA Online.

Soort persoonsgegevens:

Digitaal Vlaanderen verwerkt naast alle persoonsgegevens die in het kader van bovenstaande dienst(en) verwerkt worden ook:

a. het INSZ-nummer van de persoon bij de opdrachtgevende instantie die het bericht verstuurd

Duur van de verwerking:

Voor auditdoeleinden wordt het verzonden document met inbegrip van de metadata over iedere individuele transactie bewaard door Digitaal Vlaanderen, dit conform de afspraken tussen de opdrachtgevende instantie en de aanbieder van de eBox. Deze logdata kan enkel worden ingezien of opgevraagd door de opdrachtgevende instantie.

Het/de verzonden document(en), persoonsgegevens in het kader van bovenstaande diensten en de metadata over iedere individuele transactie (met inbegrip van de unieke identificator van de bestemmeling) worden gedurende 10 jaar bewaard in een logdatabank die enkel voor de opdrachtgevende instantie toegankelijk is.

Categorieën van betrokkenen:

Het betreft zowel de burgers naar wie de opdrachtgevende instantie een document wenst te sturen via de eBox voor natuurlijke personen, als de ondernemingen waarnaar de opdrachtgevende instantie een document wenst te sturen via de eBox voor ondernemingen.

Afgenomen diensten

De verwerkingsopdracht omvat volgende afgenomen diensten:

API-aansluiting MAGDA documentendienst:

- ☐Aansluiting eBox voor natuurlijke personen
- ☐Aansluiting eBox voor ondernemingen
- ☐Aansluiting print- en leverdienstenleverancier
- ☒Digitaal Vlaanderen als document provider

Aansluiting MAGDA documentendienst via MAGDA Online:

- ☐Aansluiting eBox voor natuurlijke personen
- ☐Aansluiting eBox voor ondernemingen
- ☐Aansluiting print- en leverdienstenleverancier
- ☒Digitaal Vlaanderen als document provider
- ☒Bezorgen van de documenten via MAGDA Online

BIJLAGE 2: ONDERVERWERKER(S)

Digitaal Vlaanderen doet beroep op volgende onderverwerker(s) voor de verwerking van persoonsgegevens zoals uiteengezet in deze verwerkersovereenkomst:

- **CRONOS PUBLIC SERVICES NV** een vennootschap die is opgericht en bestaat onder de wetgeving van België, met ondernemingsnummer 0458.085.765, waarvan de statutaire zetel zich bevindt op Veldkant 33 bus A, 2550 Kontich, België.

Enkel indien ook gebruik gemaakt wordt van print- en leverdiensten:

- **IPEX NV** een vennootschap die is opgericht en bestaat onder de wetgeving van België, met ondernemingsnummer 0429.119.090, waarvan de statutaire zetel zich bevindt op Landaslaan 5, 1480 Sint-Renelde.

Enkel indien ook gebruik gemaakt wordt van MAGDA Online:

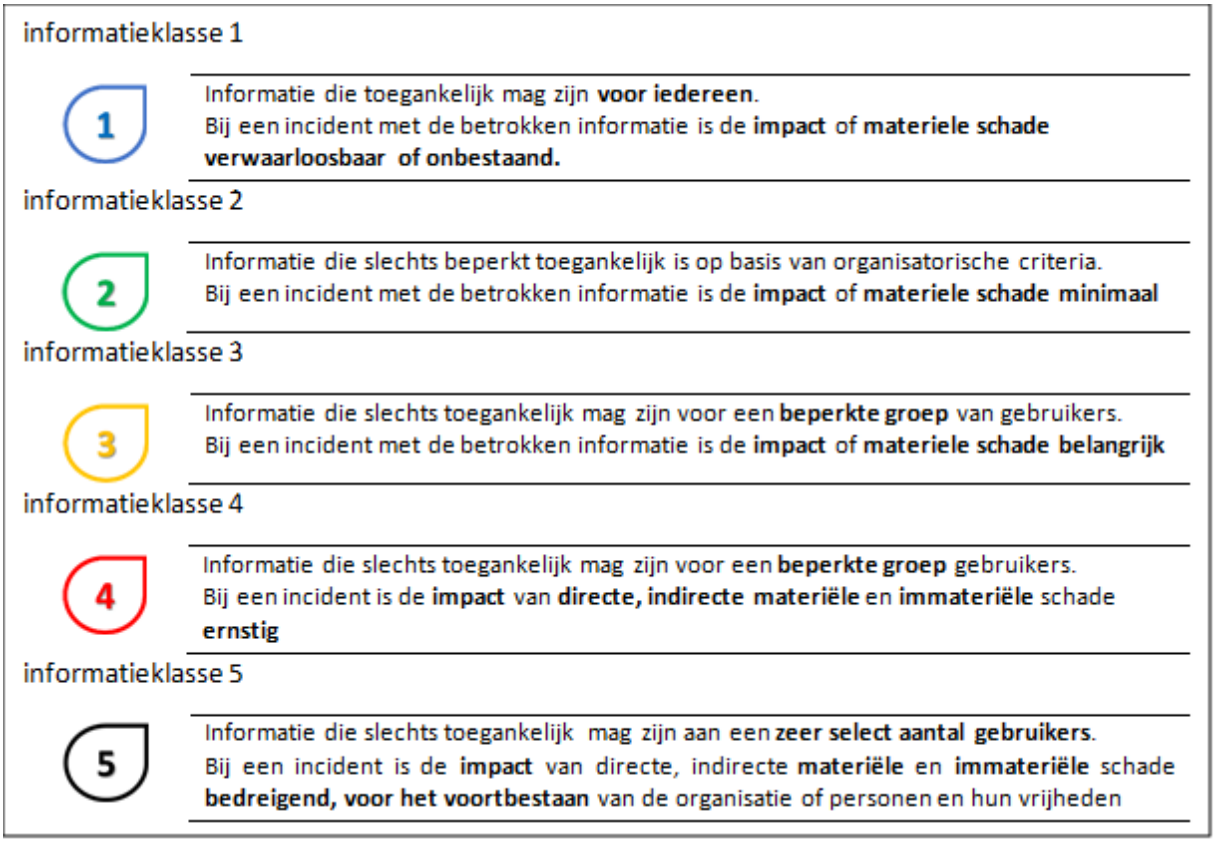
- **AMAZON WEB SERVICES EMEA SARL,** een vennootschap opgericht onder Luxemburgs recht.

Wanneer bijkomende onderverwerkers worden aangesteld of indien de samenwerking met een onderverwerker wordt stopgezet, zal deze bijlage worden aangepast overeenkomstig artikel 7 van deze verwerkersovereenkomst.

BIJLAGE 3: TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

1. Veiligheidskader

Digitaal Vlaanderen maakt gebruik van de informatieclassificatie van de Vlaamse overheid als kompas voor het implementeren van de nodige technische en organisatorische maatregelen om het beveiligingsniveau van de verwerking te waarborgen, hierbij rekening houdende met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen:



De classificatie die van toepassing is, is de hoogste classificatie die uit de inventaris van alle geïdentificeerde persoonsgegevens kan afgeleid worden. Het is die classificatie die de informatieclassificatie van het volledige platform bepaalt. De gegevens die via de MAGDA Documentendienst verwerkt worden, zijn na analyse volgens dit model ingedeeld in informatieklasse 4.

Om de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens tijdens de verwerking te garanderen worden, op basis van deze indeling, de hierna beschreven technische en organisatorische veiligheidsmaatregelen genomen.

2. Organisatorische veiligheidsmaatregelen

a. Op niveau van het agentschap Digitaal Vlaanderen

- Er is een functionaris voor gegevensbescherming aangesteld. De functionaris voor gegevensbescherming controleert of de verwerkingen gebeuren in overeenstemming met de bepalingen van de algemene verordening gegevensbescherming (AVG), met de bepalingen van de federale en Vlaamse regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens en met de verwerkersopdracht.
- Het Digitaal Vlaanderen beschikt over een informatieveiligheidsbeleid en –plan.
- Conform de AVG:
    - Wordt een geheimhoudingsverklaring ondertekend door alle relevante interne en externe medewerkers, inclusief onderverwerkers;
    - Is er een incidentenbeheerprocedure opgesteld en naar alle relevante medewerkers gecommuniceerd;
    - Zijn er procedures opgesteld en gecommuniceerd naar alle relevante medewerkers met betrekking tot volgende aspecten:
        - Recht van inzage,
        - Recht op rectificatie,
        - Recht op gegevenswissing,
        - Recht op beperking van de verwerking,
        - Recht op overdraagbaarheid van de persoonsgegevens,
        - Recht van bezwaar;
- Maatregelen zijn getroffen voor de fysieke beveiliging van de omgeving.

b. Specifiek voor de MAGDA documentendienst

- Conform de AVG:
    - Is er een register van verwerkingen opgesteld;
    - Beschikt de privacylogging over een auditfunctionaliteit die toegankelijk is voor de functionaris voor gegevensbescherming van Digitaal Vlaanderen.
    - Processen zijn uitgeschreven en geïmplementeerd met betrekking tot het toegangsbeheer, het loggingsbeheer, het security event management.
- In lijn met de verwerkersovereenkomst zijn verplichtingen inzake de verwerking van persoonsgegevens contractueel vastgelegd met de respectieve onderverwerkers.
- Een regelmatige security audit wordt minstens één keer per drie jaar uitgevoerd door een onafhankelijke, ISO27001-gecertifieerde instantie.

c. Specifiek voor MAGDA Online

- MAGDA Online is uitvoering gedocumenteerd voor interne doeleinden op Confluence, Azure Devops en SharePoint
- Conform de AVG:
    - Is er een register van verwerkingen opgesteld;
    - Beschikt de privacylogging over een auditfunctionaliteit die toegankelijk is voor de functionaris voor gegevensbescherming van de opdrachtgevende instantie.
    - Processen zijn uitgeschreven en geïmplementeerd met betrekking tot het toegangsbeheer, het loggingsbeheer, het security event management.

  In lijn met de verwerkersovereenkomst zijn verplichtingen inzake de verwerking van persoonsgegevens contractueel vastgelegd met de respectieve onderverwerkers.

3. Technische veiligheidsmaatregelen

a. Specifiek voor de MAGDA documentendienst

i. Least privileged principe bij het toekennen van functioneel noodzakelijke toegangen

- Het Least privileged principe wordt bewaakt door een aangestelde toegangsbeheerder.

1. Verzender

- De opdrachtgevende instantie kan slechts documenten van een bepaalde categorie van persoonsgegevens versturen voor zover de opdrachtgevende instantie gemachtigd is voor het versturen van deze persoonsgegevens.
- De opdrachtgevende instantie kan slechts persoonsgegevens aangaande een bepaalde persoon versturen voor zover deze een dossier van deze persoon in behandeling heeft en daarvoor gemachtigd is.

2. Systeembeheerder

- Het toegangsbeheer wordt ingeregeld door middel van een security matrix. Deze maakt onderscheid tussen de verschillende componenten, rollen en granulariteit van toegangen (lezen, schrijven, wijzigen).
- De toegangen worden per rol bepaald op basis van de minimale autorisatie noodzakelijk in functie van de uitvoering van de taak.

3. Applicatie

- De verschillende componenten hebben elk dedicated credentials nodig om te functioneren en toegang te vragen tot andere componenten en externe bronnen.
- Communicatie tussen componenten binnen het platform verloopt steeds over HTTPS.

ii. Encryptie ter afscherming van de persoonsgegevens

- Communicatie tussen partijen verloopt steeds over TLS.
- De connectie met en de toegang tot de MAGDA documentendienst gebeurt altijd op basis van authenticatie via certificaten.
- Deze certificaten worden afgeleverd door het Digitaal Certificatenbeheer platform van de Vlaamse overheid (VODCBaaS), gekoppeld aan het Toegangs- en gebruikersbeheer van de Vlaamse overheid (via de Federal Authentication Service – FAS) of via een andere Certificate Authority.
- De toegangsbeveiliging voor externe applicaties is ingeregeld via de Autorisatie server van Digitaal Vlaanderen en de controles via een Policy Enforcement Point van het API-beheerplatform APIGEE.
- Communicatie tussen Digitaal Vlaanderen en de onderverwerker Cronos Public Services verloopt steeds via een beveiligde site-to-site VPN-tunnel (IPSEC).
- Enkel geautoriseerde medewerkers van Digitaal Vlaanderen kunnen certificaten beheren.
- De certificatenbeheerder is niet de ontwikkelaar of operator zelf.
- Digitaal Vlaanderen heeft de volledige controle over de levenscyclus van de eigen certificaten.
- Alle documenten en metadata die door de MAGDA documentendienst worden behandeld worden altijd in een versleutelde opslag bewaard.

iii. Logging

- Diverse aspecten van de MAGDA documentendienst worden gelogd om verschillende redenen:
    - Technische logging van de beschikbaarheid en performantie van de onderliggende infrastructuur met het oog op bedrijfszekerheid;
    - Traffic logging van alle transacties die via de MAGDA documentendienst verlopen met het oog op probleem- en incidentanalyse;
    - Privacylogging voor auditing doeleinden van alle transacties die via de MAGDA documentendienst verlopen in lijn met de wettelijke bepalingen en best practices (wie heeft welk gegeven op welk tijdstip geraadpleegd over wie en met welke finaliteit).

b. Specifiek voor MAGDA Online

i. Hosting – privacy by design

- MAGDA Online wordt in de AWS-cloud gehosted. Het "AWS GDPR DATA PROCESSING ADDENDUM", welke de verwerkingsovereenkomst tussen Cronos Public Services NV en AWS uitmaakt, kan worden teruggevonden op de website van AWS [https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf].
- een studie werd uitgevoerd voor de veilige inrichting van MAGDA Online op AWS, rekening houdend met de vereisten van de informatieklasse 4. Resultaat van deze studie zijn design documenten voor applicatie management, architectuur, DevOps, en security.
- Digitaal Vlaanderen heeft binnen het MAGDA Onlineteam een voorstudie uitgevoerd waarbij de design veiligheidsaspecten technisch uitgewerkt zijn.
- Digitaal Vlaanderen heeft vanuit de MAGDA Online architectuur werkgroep volgende AWS referentie architecturen als basis design vooropgesteld:
    - AWS VPC Architecture
    - AWS standardized architecture for NIST high-impact controls

ii. Data Privacy Impact Assessment (DPIA)

- De functionaris voor gegevensbescherming van Digitaal Vlaanderen heeft in nauwe samenwerking met het MAGDA Online team een Data Privacy Impact Assessment oefening doorgevoerd.

iii. Enkel functioneel noodzakelijke toegangen

1. Medewerker van een opdrachtgevende instantie

- kan enkel zijn eigen gegevens inzien na authenticatie via toegangsbeheer (ACM) met eIDAS betrouwbaarheidsniveau "High" of "Substantial"
- Kan zich authentiseren via de FAS middelen hiervoor beschikbaar.

2. Beheerder

- wordt geauthentiseerd middels 2 factor identificatie via AWS Multi-Factor Authentication
- wordt geautoriseerd middels gesloten doelgroepen via AWS Identity and Access Management (IAM) rollen.

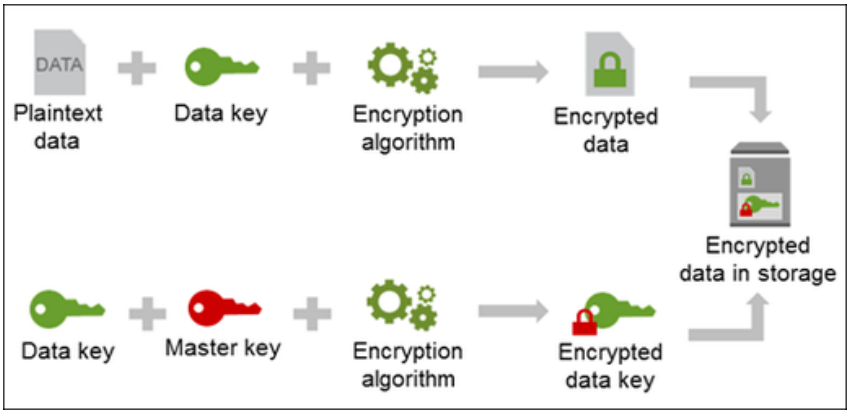
- Het functie gescheiden beheer van deze gesloten doelgroepen gebeurt middels AWS Identity and Access Management (IAM).

3. Applicatie (proces & systeem)

- De verschillende applicatie-onderdelen hebben elk dedicated AWS credentials nodig om te functioneren en toegang te vragen tot andere applicatie onderdelen, databanken & externe bronnen.
- Via AWS Identity and Access Management (IAM) beveiligen we deze functionaliteiten via "gesloten doelgroepen" en bijhorende policies opdat elk applicatie onderdeel enkel toegang krijgt tot de resources die nodig zijn om correct te functioneren.

iv. Encryptie ter afscherming van de data naar systeembeheerders toe

- De data in alle databanken alsook in hun afgeleide back-ups, lees kopijen & snapshots zijn versleuteld met het AES-256 encryptie algoritme.
- Het resultaat is dat de neergeschreven data ("data at rest") steeds geëncrypteerd is. Systeembeheerders kunnen de data niet onversleuteld raadplegen.
- Voor het aanmaken en beheren van de sleutels alsook het uitvoeren van de encryptie bewerking maken we gebruik van de AWS Key Management Service (AWS KMS) en het "envelope encryption" principe waarbij de Master key separaat van de encrypted data wordt opgeslagen.



v. Encryptie ter afscherming van onderschepping van gegevens tijdens het transport over het netwerk

Browser **MAGDA Online** **MAGDA**

- Communicatie tussen browser & MAGDA Online verloopt steeds over HTTPS
- Communicatie tussen MAGDA Online en de Magda documentendienst verloopt volgens de beveiligingsstandaarden van de MAGDA documentendienst.

vi. Encryptie sleutelbeheer

- Digitaal Vlaanderen stelt de beheerder aan van de omgeving en van de toegangen tot de omgeving en de encryptie sleutels.
- De beheerder is niet de ontwikkelaar of operator zelf.
- De beheerder bepaalt de toegangen op basis van het least privilege principe.
- Digitaal Vlaanderen voert het sleutelbeheer uit gebruik makend van de KMS infrastructuur om een volledige "separation of duties" (functiescheiding) te realiseren.
- Digitaal Vlaanderen heeft de volledige controle over de levenscyclus, het key rotatie proces en de duurzaamheid van de master sleutels die separaat van de versleutelde data opgeslagen worden.
- Enkel geautoriseerde gebruikers van Digitaal Vlaanderen kunnen de sleutels beheren.
- Digitaal Vlaanderen monitoring proces via het opvolgen van AWS Cloudtrail logs & CloudWatch events binnen het Digitaal Vlaanderen SoC.

vii. Monitoring en opvolging

- Wie, wanneer, welk request type, op welke resource uitgevoerd heeft wordt als events gelogd op AWS Cloudtrail.
- Deze events zijn afkomstig van API-oproepen, AWS SDK-oproepen, oproepen van command line tools alsook events van AWS dienst specifieke acties.
- Zo worden ook de authenticaties & autorisaties van AWS IAM gelogd voor accounting doeleinden.
- Deze logging wordt historisch raadpleegbaar bijgehouden wat beveiligingsanalyse, tracking van bronwijziging en audit daarvan vereenvoudigt.
- Digitaal Vlaanderen Security Operations Center (SoC) processen worden ingericht voor opvolging
- SIEM via AWS Cloudwatch (Root account toegang & master key beheer)
- Manuele opvolging AWS Audit log (Cloudtrail) + configuratie van extra Cloudwatch events "on the job"

viii. Privileged access management (PAM)

- De MAGDA Online PAM beheerprocessen zijn in kaart gebracht en zowel functioneel als technisch beschreven.
- De MAGDA Online PAM-processen zijn technisch ingericht gebruik makend van AWS platform diensten (AWS IAM).
- Audit logs van deze PAM processen zijn beschikbaar via AWS CloudTrail.
- Standaard AWS PAM implementatie
- 2-factor authenticatie
- Least privileged principe via AWS IAM

ix. Veiligheidscontroles

- Interne security regressie testen
    - Code vulnerability OWASP checks, continu ingeregeld via code build & release pipelines
- Externe security testen
    - Statische code vulnarability scan (Source Code Review) zijn recurrent ingepland
    - Dynamische penetration testen zijn recurrent ingepland
- Externe applicatie architectuur analyse
    - CATA – een Comprehensive Application Threat Analysis is uitgevoerd