

**PROTOCOL VOOR DE ELEKTRONISCHE MEDEDELING VAN PERSOONSGEGEVENS
TUSSEN AGENTSCHAP WEGEN EN VERKEER [INSTANTIE 1] EN DE LIJN [INSTANTIE 2]**

in het kader van MOBILIDATA – doorstroming openbaar vervoer

[22/01/2024]

Dit protocol wordt gesloten conform artikel 8, §1, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer.

TUSSEN

(VLAAMSE GEMEENSCHAP) of (VLAAMS GEWEST), vertegenwoordigd door de Vlaamse Regering, bij delegatie, in de persoon van de leidend ambtenaar van agentschap zonder rechtspersoonlijkheid Agentschap Wegen en Verkeer, administrateur-generaal Kathy Vandenmeersschaut

ingeschreven in het KBO met nummer 0316.380.841, waarvan de administratieve zetel zich bevindt te Koning Albert II-laan 20 bus 4, 1000 Brussel.

hierna: “INSTANTIE 1”;

EN

De Vlaamse Vervoermaatschappij De Lijn, een publiekrechtelijk vormgegeven extern verzelfstandigd agentschap met maatschappelijke zetel te 2800 Mechelen, Motstraat 20, en ingeschreven in de kruispuntbank der ondernemingen onder het nummer (RPR Antwerpen, afdeling Mechelen) 0242.069.537, hierbij vertegenwoordigd door mevrouw Ann Schoubs, Directeur-Generaal

hierna: “INSTANTIE 2”;

[INSTANTIE 1] en [INSTANTIE 2] worden hieronder ook wel afzonderlijk aangeduid als een “partij” of gezamenlijk als de “partijen”;

NA TE HEBBEN UITEENGEZET

- A. [INSTANTIE 1] is het agentschap dat is opgericht voor de uitvoering van het beleid inzake wegeninfrastructuur en elektromechanische uitrustingen. Het AWW beheert ca. 7.000 km gewest- en autosnelwegen en ruim 7.700 km fietspaden. De missie van AWW bestaat erin om, binnen het beleidsdomein Mobiliteit en Openbare Werken, te zorgen voor de uitvoering van de investeringswerken aan de gewestwegen en voor de ondersteuning op het gebied van elektriciteit, mechanica en telematica-uitrusting voor het beleidsdomein Mobiliteit en Openbare Werken. Tevens is het AWW verantwoordelijk voor het onderhoud en de exploitatie van deze infrastructuur, evenals voor het operationele beheer van het verkeer en het vervoer over die wegen.;

- B. [INSTANTIE 2] is binnen het beleidsdomein Mobiliteit en Openbare Werken een publiekrechtelijk vormgegeven extern verzelfstandigd agentschap met maatschappelijke zetel te 2800 Mechelen, Motstraat 20 en ingeschreven in de kruispuntbank der ondernemingen onder het nummer (RPR Antwerpen, afdeling Mechelen) 0242.069.537. De Lijn is de partner van het Vlaams Gewest voor het stedelijk en regionaal openbaar vervoer in, van en naar Vlaanderen.
- C. Mobilidata is een programma van de Vlaamse overheid met ondersteuning van Imec. Meerdere Vlaamse overheidsinstellingen hebben hun schouders onder dit programma gezet, zijnde: Departement Mobiliteit en Openbare Werken (MOW), Agentschap Wegen en Verkeer (AWV), Departement Economie, Wetenschap en Innovatie (EWI) en het Agentschap Innoveren en ondernemen (Vlaio). Het programma wordt mogelijk gemaakt dankzij funding van Vlaio en met steun van CEF (Connecting Europe Facility).

Mobilidata beoogt een platform dat slimme ICT-systemen, ingebouwd in de nieuwe wegeninfrastructuur, connecteert met weggebruikers. Het Agentschap Wegen en Verkeer heeft als opdracht gekregen dit “Mobilidata” platform te ontwerpen, aan te leggen, te onderhouden, en om de elektromechanische en telematica-uitrustingen te beheren en technisch te exploiteren.

Het programma Mobilidata realiseert een netwerk van duurzame, slimme en betrouwbare data. Via boordcomputers of smartphones is het mogelijk voor weggebruikers om te communiceren met de geconnecteerde systemen. De slimme infrastructuur die Mobilidata voorziet, combineert de informatie van de weggebruiker met andere realtime data. Op die manier kunnen bijvoorbeeld verkeerslichten beter op de mobiliteitsbehoeftes van de actieve weggebruikers inspelen. In de andere richting kan de weggebruiker sneller en gericht geïnformeerd worden over de verkeerssituatie.

Het programma Mobilidata bestaat uit verschillende nieuwe toepassingen die bijdragen tot een vlotter, duurzamer, meer comfortabel en veiliger verkeer.

De realisatie van Mobilidata kent vijf belangrijke assen:

1. Verkeersregels: Weggebruikers informeren over de verkeersregels met zowel statische als dynamische informatie;
2. Risico & gevaar: Weggebruikers informeren over de nabije verkeerssituatie zoals trage voertuigen, ongevallen, pannes, hulpdienstvoertuigen, wegenwerken, ...;
3. Slimme verkeerslichten: Verkeersstroom op kruispunten optimaliseren en veiliger maken aan de hand van geconnecteerde, intelligente verkeersregel-installaties (iVRIs);
4. Navigatie en parkeermanagement: Weggebruikers informeren over geadviseerde routes, parkeergelegenheid voor vrachtwagens, of over Park & Ride faciliteiten;
5. Beleidsondersteuning: Historische database opbouwen en ter beschikking stellen aan het MOW, AWV en lokale wegbeheerders om bestaande beleidsregels bij te stellen of nieuwe beleidsregels in te voeren.

Om bovenstaande assen uit te werken heeft AWV tijdens de onderzoeksfase van Mobilidata 29 use cases gedefinieerd. Deze use cases zijn beschreven in bijlage [M001].

Om deze nieuwe of verbeterde diensten aan de weggebruikers te kunnen verlenen, rekent [INSTANTIE 1] op de aansluiting van en gegevensuitwisseling met service providers. Deze service providers leveren verkeersinformatiediensten aan hun aangesloten weggebruikers of partners.

[INSTANTIE 2] is in de context van dit protocol een deelnemer en gebruiker van smart mobility diensten uit het Mobilidata portfolio.

C2. VOORSTELLING VAN HET VERLOOP VAN DE GEPLANDE GEGEVENSSTROMEN.

Dit protocol heeft betrekking op de gegevensstromen die [INSTANTIE 1] en [INSTANTIE 2] uitwisselen als verwerkingsverantwoordelijken.

De gegevensstromen vallen uiteen in volgende grote stromen:

1. Verkeersinformatie-berichtenstroom van Mobilidata Interchange van [INSTANTIE 1] naar Back-end van De Lijn van [INSTANTIE 2]
 2. Prioriteitsaanvragen-stroom [SREMs, SSEMS en CAMs] van Back-end van De Lijn van [INSTANTIE 2] naar Mobilidata Interchange van [INSTANTIE 1] en omgekeerd
- D. De partijen wensen overeenkomstig artikel 8, §1, van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer een protocol te sluiten met betrekking tot de elektronische mededeling van persoonsgegevens. Dat protocol wordt bekendgemaakt op de website van beide partijen.
- F. De functionaris voor gegevensbescherming van [INSTANTIE 1] heeft in de periode oktober 2023 t.e.m. maart 2024 adviezen met betrekking tot een ontwerp van dit protocol gegeven.
- G. De functionaris voor gegevensbescherming van [INSTANTIE 2] heeft in de periode oktober 2023 t.e.m. maart 2024 adviezen met betrekking tot een ontwerp van dit protocol gegeven.

WORDT OVEREENGEKOMEN WAT VOLGT:

Artikel 1: Onderwerp

In dit protocol worden de voorwaarden en modaliteiten van de elektronische mededeling van de (persoons)gegevens zoals omschreven in artikel 3 tussen [INSTANTIE 1] en [INSTANTIE 2] uiteengezet.

Artikel 2: Rechtvaardigingsgronden van zowel de mededeling als de inzameling van de (persoons)gegevens

Artikel 2.1: Beoogde verwerking door [INSTANTIE 2] van Verkeersinformatie-berichtenstroom (Gegeven 1)

De beoogde gegevensverwerking door [INSTANTIE 2] gebeurt op grond van

- Artikel 6.1.e AVG (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) voor de verwerkingen ter bevordering van de doorstroming;

In dat verband kan verwezen worden naar de verplichtingen opgenomen in artikel 7 Decreet betreffende de basisbereikbaarheid en artikel 19 van haar Uitvoeringsbesluit (Besluit van de Vlaamse Regering van 4 september 2020 tot bepaling van de kwaliteitseisen voor het kernnet en het aanvullend net en de streefwaarden voor wegbeheerders inzake de doorstroming van het openbaar vervoer) evenals artikel 4 van het Decreet betreffende de basisbereikbaarheid.

Artikel 6.1.f AVG (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):

- gerechtvaardigd vanwege het recht op “veiligheid” voor de bij [INSTANTIE 2] aangesloten gebruikers (omdat de verkeersinformatie de gebruikers toelaat te anticiperen op risicovolle verkeerssituaties)
- de verwerking is noodzakelijk omdat zonder de gegevens geen waarschuwingen over de verkeerssituaties kunnen worden uitgestuurd
- m.b.t. de afweging van het recht op privacy van de betrokken chauffeurs (hulpdiensten, traag rijdende voertuigen) en het recht op veiligheid van de aangesloten weggebruikers wordt geoordeeld dat het recht op veiligheid belangrijker is. Bijkomend wordt de veiligheid van de betrokken chauffeurs zelf ook verhoogd door het verspreiden van waarschuwingen m.b.t. de verkeersrisico's van hun verplaatsing.
- [INSTANTIE 1] maakte dezelfde afweging m.b.t. het uitsturen van deze gegevens in het kader van haar taak van algemeen belang.

[INSTANTIE 1] heeft de opgevraagde gegevens oorspronkelijk verzameld voor volgende doeleinden:

- het leveren en verbeteren van verkeersinformatiediensten aan weggebruikers
- Verdere verwerking: het aggregeren en daarna archiveren voor verder onderzoek en beleidsevaluatie

[INSTANTIE 2] zal de opgevraagde gegevens verwerken voor volgende doeleinden:

- het leveren en verbeteren van verkeersinformatiediensten aan chauffeurs in de voertuigen van De Lijn en onderaannemers

Het doeleinde van de verdere verwerking van deze persoonsgegevens door [INSTANTIE 2] is verenigbaar met de doeleinden waarvoor [INSTANTIE 1] de gegevens oorspronkelijk heeft verzameld, gezien het doeleinde identiek is.

Artikel 2.2: Beoogde verwerking door [INSTANTIE 1] van Prioriteitsaanvragen (Gegeven 2)

De beoogde gegevensverwerking door [INSTANTIE 1] gebeurt op grond van

- Artikel 6.1c Wettelijke verplichting: Decreet Basisbereikbaarheid, art 47§2

[INSTANTIE 1] zal de opgevraagde gegevens verwerken voor volgende doeleinden:

- Het verlenen van conditionele prioriteit aan specifieke weggebruikers op geconnecteerde kruispunten.

- Het optimaliseren en verbeteren van verkeersregelingen op kruispunten
- Het leveren en verbeteren van verkeersinformatiediensten
- Verdere verwerking: het aggregeren en daarna archiveren voor verder onderzoek en beleidsevaluatie

Artikel 3: De gevraagde (persoons)gegevens en de categorieën en omvang van de gevraagde (persoons)gegevens conform het proportionaliteitsbeginsel: Gegeven 1 en Gegeven 2

Artikel 3.1: Gegeven 1

In onderstaande tabel wordt een overzicht gegeven van de verschillende persoonsgegevens die worden meegedeeld van [INSTANTIE 1] naar [INSTANTIE 2], alsook de verantwoording van de proportionaliteit en de bewaartermijn van de gegevens.

Het betreft geen persoonsgegevens als vermeld in artikel 9 en/of 10 van de algemene verordening gegevensbescherming. Indien dat wel het geval is, wordt dit gespecificeerd in onderstaande tabel.

Gegeven 1: Verkeersinformatie-berichtenstroom	Persoonsgegevens in de Verkeersinformatie-berichtenstroom zijn: - Real-time verplaatsingsgegevens van prioritaire voertuigen en (indien gekend) type van prioritair voertuig. - Real-time verplaatsingsgegevens van traag rijdende of stilstaande voertuigen - Real-time verplaatsingsgegevens van dienstvoertuigen tijdens interventies of werkzaamheden en type van dienstvoertuig - Positiegegevens van mogelijke spookrijders Overige gegevens hebben betrekking op gebeurtenissen op het wegennet, maar worden niet als persoonsgegevens geclassificeerd.
Verantwoording proportionaliteit	- Het uitwisselen van real-time verplaatsingsgegevens van prioritaire voertuigen is noodzakelijk om andere weggebruikers voor de komst en/of aanwezigheid van deze voertuigen te waarschuwen. - Het uitwisselen van real-time verplaatsingsgegevens van traag rijdende voertuigen, stilstaande voertuigen of spookrijders is noodzakelijk om andere weggebruikers voor de aanwezigheid van dit mogelijke gevaar te waarschuwen. - Het uitwisselen van real-time verplaatsingsgegevens van dienstvoertuigen is noodzakelijk om andere weggebruikers voor de interventies of werkzaamheden te waarschuwen.

De meegedeelde gegevens (Gegeven 1) kunnen door [INSTANTIE 2] gedurende maximum 6 maanden bewaard worden. Indien het mogelijk is om de medegedeelde gegevens sneller te verwijderen, zal dat gebeuren. Deze bewaartermijn kan worden verantwoord gezien de noodzaak voor het bijhouden voor de analyse en het verbeteren van de service.

Artikel 3.2: Gegeven 2

In onderstaande tabel wordt een overzicht gegeven van de verschillende gegevens die worden meegedeeld van [INSTANTIE 2] naar [INSTANTIE 1], alsook de verantwoording van de proportionaliteit en de bewaartermijn van de gegevens

De classificatie van de gegevens na doorgifte van [INSTANTIE 2] naar [INSTANTIE 1] is op dit moment niet duidelijk. Hiervoor verwijzen we naar de Case T-557/20 Single Resolution Board (SRB) vs European Data Protection Supervisor (EDPS) en het beroep hiertegen in Case C-413/23 P.

Ongeacht de classificatie, zal [INSTANTIE 1] de ontvangen gegevens behandelen alsof het persoonsgegevens betreft.

Gegeven 2 Prioriteitsaanvragen- stroom [SREMs, SSEMs en CAMs]	Prioriteitsaanvragen-stroom [SREMs, SSEMs en CAMs] bevat volgende gegevens: - Real-time verplaatsingsgegevens van voertuigen van De Lijn of onderaannemers waarvoor prioriteit wordt aangevraagd op een geconnecteerd kruispunt [CAMs] - Type en Rol van de betrokken voertuigen - Konvooi-informatie van de betrokken voertuigen - Aanvragen van prioriteit voor een beweging op het kruispunt met inschatting van aankomsttijd [SREMs] - Antwoorden op de aanvragen van prioriteit [SSEMs] - In de toekomst kan deze berichtenstroom ook bijkomende gegevens bevatten m.b.t. authenticatie van de aanvrager (bv. certificaten)
Verantwoording proportionaliteit	De verwerking van de gegevens is noodzakelijk voor geconnecteerde verkeersregelininstallaties om prioriteit te verlenen aan specifieke geconnecteerde weggebruikers of voor het in zijn geheel doorlaten van aangemelde konvoeien.

De meegedeelde gegevens zullen door [INSTANTIE 1] bewaard worden volgens onderstaande tabel. Deze bewaartermijnen worden verder geëvalueerd en indien mogelijk verkort, indien noodzakelijk verhoogd.

Gegeven	Maximale bewaartermijn	Verantwoording
Gegeven 2 Prioriteitsaanvragen-stroom [SREMs, SSEMs en CAMs]	18 maanden	18 maanden worden ingeschat als nodig voor het analyseren verbeteren en verzekeren van het goed verlenen van prioriteit op kruispunten, zodat een vergelijkingen en evoluties over een jaar heen kunnen worden gemaakt.

Artikel 4: De categorieën van ontvangers en derden die mogelijks de (persoons)gegevens, vermeld in artikel 3, eveneens verkrijgen

Artikel 4.1: Door [INSTANTIE 1]

[INSTANTIE 1] zal de meegedeelde gegevens in het kader van de in artikel 2, 2°, vooropgestelde finaliteiten kunnen meedelen aan volgende categorie(ën) van ontvangers:

- Enkel personen van [INSTANTIE 1] die omwille van hun functie deze informatie nodig hebben voor de uitvoering van hun werk, krijgen toegang tot de informatie.
- Daarnaast kunnen de gevraagde gegevens worden medegedeeld aan of ingezien door:
 - o Verwerkers van [INSTANTIE 1] – leveranciers van verkeersregelingen, verkeersinformatiediensten of externe expertise
 - o Departement Mobiliteit en Openbare Werken
 - o Lokale wegbeheerders (voor de gegevens op de door hen beheerde wegen)
 - o [INSTANTIE 2]

Elke eventuele mededeling van de gegevens door [INSTANTIE 1] moet voorafgaandelijk aan [INSTANTIE 2] worden gemeld en moet uiteraard in overeenstemming zijn met de relevante wet- en regelgeving.

Artikel 4.2: Door [INSTANTIE 2]

[INSTANTIE 2] zal de meegedeelde persoonsgegevens in het kader van de in artikel 2.1, vooropgestelde finaliteiten kunnen meedelen aan volgende categorie(ën) van ontvangers:

- Enkel personen van [INSTANTIE 2] die omwille van hun functie deze informatie nodig hebben voor de uitvoering van hun werk, krijgen toegang tot de informatie.
- Daarnaast kunnen de gevraagde gegevens worden medegedeeld aan of ingezien door:
 - o Verwerkers van [INSTANTIE 2] – leveranciers van verkeersinformatiediensten of externe expertise.

Elke eventuele andere mededeling van de gevraagde persoonsgegevens door [INSTANTIE 2] moet voorafgaandelijk aan [INSTANTIE 1] worden gemeld en moet uiteraard in overeenstemming zijn met

de relevante wet- en regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens. Dat betekent onder meer dat [INSTANTIE 2] waar vereist een protocol sluit voor de mededeling van de gevraagde gegevens.

Artikel 5. Periodiciteit van de mededeling en de duur van de mededeling

De (persoons)gegevens, vermeld in artikel 3, zullen PERMANENT tussen [INSTANTIE 1] en [INSTANTIE 2] worden uitgewisseld omdat het leveren van de diensten real-time gegevens vereist.

De (persoons)gegevens, vermeld in artikel 3, worden uitgewisseld voor onbepaalde duur.

Artikel 6: Beveiligingsmaatregelen

Volgende maatregelen worden getroffen ter beveiliging van de mededeling van de (persoons)gegevens, vermeld in artikel 3:

Artikel 6.1: Beveiligingsmaatregelen door [INSTANTIE 1]

- Encryptie van alle verbindingen waarover persoonsgegevens verstuurd worden
- Encryptie van opslag
- Toegangscontrole waarbij uitgegaan wordt van het principe van minste privilege
- Wachtwoord Policy
- Vastgelegde rollen en procedures rond toegangscontrole
- Periodieke controle op toegangsrechten

Daarnaast werden ook volgende specifieke maatregelen in het kader van de gegevensmededeling getroffen:

- Bijhouden van een verwerkingsregister
- Vastleggen en minimaliseren van verwerkte velden
- Anonimisatie of pseudonimisatie waar mogelijk
- Automatische logging van toegang tot gegevens
- Toegangslogs worden zo veel mogelijk gecentraliseerd en zijn doorzoekbaar

[INSTANTIE 1] treft ten minste volgende organisatorische en technische beveiligingsmaatregelen ter beveiliging van de ontvangen gegevens bij verdere verwerking:

Algemeen

- Een algemeen beveiligingsplan wordt gevolgd om actief de beveiliging te verbeteren
- Een algemeen informatiebeveiligingsbeleid is van kracht
- Taken en rollen rond beveiliging zijn toegekend
- Alle personeelsleden van zijn gehouden tot een contractuele of statutaire vertrouwelijkheids- of geheimhoudingsplicht.

Incident Response/Service Desk

- Een incident response team wordt ingesteld.
- Incident response policy en proces zijn vastgelegd.
- Een escalatieprocedure wordt vastgelegd.

Risicobeheer

- Risico's voor een project werden vastgelegd volgens een standaard.
- Een DPIA 'Data Protection Impact Assessment' is uitgevoerd.

Privacy

- Een DPO is aangesteld.
- Gegevens zijn gecategoriseerd.
- Verwerkingsovereenkomsten worden opgemaakt met derde partijen.
- Een procedure voor het uitoefenen van rechten door betrokkenen is vastgelegd.

Fysieke Beveiliging

- Toegang gebeurt via een badgesysteem.
- Clear Desk Policy is van kracht.
- Het gebruik van uitwisselbare media is ontmoedigd via policy.

Cloudbeveiliging

- De productie omgeving staat apart van andere omgevingen.
- Een redundante productie omgeving is beschikbaar. Deze bevinden zich op verschillende fysieke plaatsen.

Human Resource

- Tijdens de tewerkstelling wordt het belang van security en privacy benadrukt.
- In het off-boarding proces zijn stappen opgenomen om ervoor te zorgen dat alle toegang tijdig ontzegd wordt.

Toegang

- Een Access Control Policy is van kracht.
- Alle binnen- en buitengaande verbindingen gebruiken een veilig protocol.
- Automatische logging van toegang tot gegevens,
- Toegang tot de productie omgeving vereist een tijdelijk token en gebruik van een VPN.
- Een password policy is van kracht.
- De autorisatie regels worden minstens per jaar nagekeken.
- Een wachtwoord policy is van kracht.

Operations

- Backups van opgeslagen gegevens worden genomen.
- Backups in rust worden geëncrypteerd.
- Een backup policy is van kracht.
- Events op de server worden gelogd.
- Events binnen applicaties worden gelogd.
- Klokken worden via ntp gesynchroniseerd.
- Updates van operationele software wordt vooraf ingepland en worden volgens een vastgelegde procedure uitgevoerd.

Cryptografie

- Een encryption policy is van kracht.
- Sleutels worden beheerd door daarvoor bevoegde personen.
- Alle communicatie met externe partijen dient te worden geëncrypteerd.

[INSTANTIE 1] moet kunnen aantonen dat de in dit artikel opgesomde maatregelen werden getroffen. Op eenvoudig verzoek van [INSTANTIE 2] moet [INSTANTIE 1] hiervan aan [INSTANTIE 2] het bewijs overmaken.

In het geval [INSTANTIE 1] voor de verwerking van de gegevens die het voorwerp zijn van voorliggend protocol, beroep doet op een verwerker (of meerdere verwerkers), doet de [INSTANTIE 1] uitsluitend beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van de Algemene Verordening Gegevensbescherming voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. [INSTANTIE 1] sluit in voorkomend geval met alle verwerkers een verwerkersovereenkomst in overeenstemming met artikel 28 van de algemene verordening gegevensbescherming. Partijen bezorgen elkaar een overzicht van de verwerkers die de gevraagde gegevens verwerken, en actualiseren dit overzicht zo nodig.

Artikel 6.2: Beveiligingsmaatregelen door [INSTANTIE 2]

- Encryptie van alle verbindingen waarover persoonsgegevens verstuurd worden
- Encryptie van opslag
- Toegangscontrole waarbij uitgegaan wordt van het principe van minste privilege
- Wachtwoord Policy
- Vastgelegde rollen en procedures rond toegangscontrole
- Periodieke controle op toegangsrechten
- Daarnaast werden ook volgende specifieke maatregelen in het kader van de gegevensmededeling getroffen:
- Bijhouden van een verwerkingsregister
- Vastleggen en minimaliseren van verwerkte velden
- Anonimisatie of pseudonimisatie waar mogelijk
- Automatische logging van toegang tot gegevens
- Toegangslogs worden zo veel mogelijk gecentraliseerd en zijn doorzoekbaar

[INSTANTIE 2] treft ten minste volgende organisatorische en technische beveiligingsmaatregelen ter beveiliging van de ontvangen gegevens bij verdere verwerking:

Algemeen

- Een algemeen beveiligingsplan wordt gevolgd om actief de beveiliging te verbeteren
- Een algemeen informatiebeveiligingsbeleid is van kracht
- Taken en rollen rond beveiliging zijn toegekend
- Alle personeelsleden van zijn gehouden tot een contractuele of statutaire vertrouwelijkheids- of geheimhoudingsplicht.

Incident Response/Service Desk

- Een incident response team wordt ingesteld.
- Incident response policy en proces zijn vastgelegd.
- Een escalatieprocedure wordt vastgelegd.

Risicobeheer

- Risico's voor een project werden vastgelegd volgens een standaard.
- Een DPIA 'Data Protection Impact Assessment' is uitgevoerd.

Privacy

- Een DPO is aangesteld.
- Gegevens zijn gecategoriseerd.
- Verwerkingsovereenkomsten worden opgemaakt met derde partijen.
- Een procedure voor het uitoefenen van rechten door betrokkenen is vastgelegd.

Fysieke Beveiliging

- Toegang gebeurt via een badgesysteem.
- Clear Desk Policy is van kracht.
- Het gebruik van uitwisselbare media is ontmoedigd via policy.

Cloudbeveiliging

- De productie omgeving staat apart van andere omgevingen.
- Een redundante productie omgeving is beschikbaar. Deze bevinden zich op verschillende fysieke plaatsen.

Human Resource

- Tijdens de tewerkstelling wordt het belang van security en privacy benadrukt.
- In het off-boarding proces zijn stappen opgenomen om ervoor te zorgen dat alle toegang tijdig ontzegd wordt.

Toegang

- Een Access Control Policy is van kracht.
- Alle binnen- en buitengaande verbindingen gebruiken een veilig protocol.
- Automatische logging van toegang tot gegevens,
- Toegang tot de productie omgeving vereist een tijdelijk token en gebruik van een VPN.
- Een password policy is van kracht.
- De autorisatie regels worden minstens per jaar nagekeken.
- Een wachtwoord policy is van kracht.

Operations

- Backups van opgeslagen gegevens worden genomen.
- Backups in rust worden geëncrypteerd.
- Een backup policy is van kracht.
- Events op de server worden gelogd.
- Events binnen applicaties worden gelogd.
- Klokken worden via ntp gesynchroniseerd.
- Updates van operationele software wordt vooraf ingepland en worden volgens een vastgelegde procedure uitgevoerd.

Cryptografie

- Een encryption policy is van kracht.
- Sleutels worden beheerd door daarvoor bevoegde personen.
- Alle communicatie met externe partijen dient te worden geëncrypteerd.

[INSTANTIE 2] moet kunnen aantonen dat de in dit artikel opgesomde maatregelen werden getroffen. Op eenvoudig verzoek van [INSTANTIE 1] moet [INSTANTIE 2] hiervan aan [INSTANTIE 1] het bewijs overmaken.

In het geval [INSTANTIE 2] voor de verwerking van persoonsgegevens die het voorwerp zijn van voorliggend protocol, beroep doet op een verwerker (of meerdere verwerkers), doet de [INSTANTIE 2] uitsluitend beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van de Algemene Verordening Gegevensbescherming voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. [INSTANTIE 2] sluit in voorkomend geval met alle verwerkers een verwerkersovereenkomst in overeenstemming met artikel 28 van de Algemene Verordening Gegevensbescherming. Partijen bezorgen elkaar een overzicht van de verwerkers die de gevraagde gegevens verwerken, en actualiseren dit overzicht zo nodig.

Artikel 7: Kwaliteit van de (persoons)gegevens

Zodra [INSTANTIE 1] of [INSTANTIE 2] één of meerdere foutieve, onnauwkeurige, onvolledige, ontbrekende, verouderde of overtollige gegevens in de (persoons)gegevens, vermeld in artikel 3, vaststelt (al dan niet op basis van een mededeling van de betrokkene, meldt zij dat onmiddellijk aan respectievelijk [INSTANTIE 2] of [INSTANTIE 1] die na onderzoek binnen 2 weken van de voornoemde vaststellingen de gepaste maatregelen binnen 1 maand treft en de andere partij daarvan vervolgens op de hoogte brengt.

Artikel 8: Sanctie bij niet-naleving

Onverminderd haar recht om een schadevergoeding te vorderen en in afwijking van artikel 5, 2°, kan elke partij dit protocol middels eenvoudige kennisgeving en zonder voorafgaandelijke ingebrekestelling eenzijdig beëindigen indien de andere partij deze (persoons)gegevens, vermeld in artikel 3, verwerkt in strijd met hetgeen bepaald is in dit protocol, met de Algemene Verordening Gegevensbescherming of

met andere relevante wet- of regelgeving inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens.

Artikel 9: Meldingsplichten

Partijen engageren zich in het licht van artikel 33 van de Algemene Verordening Gegevensbescherming om elkaar [via de functionarissen voor gegevensbescherming] zonder onredelijke vertraging op de hoogte te stellen van elk gegevenslek dat zich voordoet betreffende de meegedeelde gegevens met impact op beide partijen en in voorkomend geval onmiddellijk gezamenlijk te overleggen teneinde alle maatregelen te nemen om de gevolgen van het gegevenslek te beperken en te herstellen. De partijen verschaffen elkaar alle informatie die ze nuttig of nodig achten om de beveiligingsmaatregelen te optimaliseren.

Partijen brengen elkaar onmiddellijk op de hoogte van wijzigingen van wetgeving met impact op voorliggend protocol, zoals de finaliteit, proportionaliteit, frequentie, duurtijd enz. en in voorkomend geval van wijzigingen omtrent de verwerkers.

Artikel 10: Toepasselijk recht en geschillenbeslechting

Dit protocol wordt beheerst door het Belgisch recht.

Alle geschillen die voortvloeien uit of verband houden met dit protocol worden beslecht door de bevoegde rechtbank in Brussel.

Artikel 11: Inwerkingtreding en opzegging

Dit protocol treedt in werking op datum van ondertekening.

Partijen kunnen dit protocol schriftelijk opzeggen mits inachtneming van een opzegtermijn van [3 maanden].

Het protocol eindigt van rechtswege wanneer er geen rechtsgrond meer bestaat voor de gevraagde doorgifte van de (persoons)gegevens, vermeld in artikel 3.

Opgemaakt te Brussel, op 14/03/2024.

Aangezien deze overeenkomst digitaal wordt ondertekend, wordt in overeenstemming met artikel 8.20 NBW slechts één (digitaal) exemplaar van deze overeenkomst opgemaakt.

administrateur-generaal
Kathy Vandenmeersschaut

[namens INSTANTIE 1]

directeur-generaal
Ann Schoubs

[namens INSTANTIE 2]

Bijlage: M0001 - Use Case Functionele Analyse – Use Case Functional Analysis