

PROTOCOL VOOR DE ELEKTRONISCHE MEDEDELING VAN PERSOONSGEGEVENS TUSSEN
AGENTSCHAP WEGEN EN VERKEER EN YUNEX NV

in het kader van MOBILIDATA – ____ EU CEF project Helmond Antwerpen - VRI testen ARU en Truck

[26/7/2024]

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

TUSSEN

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

YUNEX NV, vertegenwoordigd door de heer Ronny Govers, Managing Director, en mevrouw Lindsay Borremans, Managing Director Finance,

ingeschreven in het KBO met nummer 0764.855.094 waarvan de administratieve zetel zich bevindt te G. Demeurslaan 132, 1654 Beersel

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 AWV beheert ca. 7.000 km gewest- en autosnelwegen en ruim 7.700 km fietspaden. De missie van AWV 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 AWV 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] Yunex NV biedt als Belgische tak van Yunex Traffic intelligente verkeersoplossingen voor stedelijke en interstedelijke mobiliteitsvraagstukken. In het kader van het EU CEF Antwerpen – Helmond project, verzorgt Yunex NV de behandeling van C-ITS prioriteitsaanvragen van fietsers en vrachtwagens op onderstaande door verkeerslichten geregelde kruispunten door middel van een koppeling met de TLEX service van het Mobilidata platform.

- P095 Kastelweg – Oosterweelsteenweg, in beheer van Lantis.
- K602 Ankerrui – Oude Leuwenrui – Hessenplein, in beheer van Stad Antwerpen
- K644 Emiel Vloorstraat – Kielsbroek) Schufstraat – Herenpolderbrug, in beheer van Stad Antwerpen.

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, AWW en lokale wegbeheerders om bestaande beleidsregels bij te stellen of nieuwe beleidsregels in te voeren.

Om bovenstaande assen uit te werken heeft AWW 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 die de link hebben met de weggebruikers.

[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.

Het overzicht van de architectuur is weergegeven in de figuur in bijlage [Mobilidata Core - Architectuur Implementatie].

De gegevensstromen vallen uiteen in volgende grote stromen:

1. Weggebruikerposities-stroom rond kruispunten [CAM en SRMX] van Mobilidata Interchange en TLEX van [INSTANTIE 1] naar [INSTANTIE 2]
2. Prioriteitsaanvragen-stroom [SREMs, SSEMS en CAMs] van Mobilidata Interchange en TLEX van [INSTANTIE 1] naar [INSTANTIE 2] 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 november 2023 t.e.m. mei 2024 adviezen met betrekking tot de template van dit protocol gegeven.
- G. De functionaris voor gegevensbescherming van [INSTANTIE 2] heeft in de periode periode 6/5/2024 t.e.m. 09/05/2024 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 persoonsgegevens zoals omschreven in artikel 3 tussen [INSTANTIE 1] en [INSTANTIE 2] uiteengezet.

Artikel 2: Rechtvaardigingsgronden van zowel de mededeling als de inzameling van de persoonsgegevens

Artikel 2.1: Beoogde verwerking door [INSTANTIE 2]

Artikel 2.1.1: Beoogde verwerking door [INSTANTIE 2] van Weggebruikerposities-stroom rond kruispunten

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

- Artikel 6.1.a, toestemming.

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

- Het leveren en verbeteren van verkeersinformatiediensten:
 - 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

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

- 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

Het doeleinde van de verdere verwerking van deze persoonsgegevens door [INSTANTIE 2] is verenigbaar met de doeleinden waarvoor [INSTANTIE 1] via [INSTANTIE 2] de gegevens oorspronkelijk heeft verzameld. De mededeling is toegelaten gezien de betrokkene hiervoor toestemming heeft gegeven.

[EN]

Het doeleinde voor de verdere verwerking is archivering in het algemeen belang en wetenschappelijk onderzoek. Op deze verwerkingen geldt een uitzondering volgens artikel 5, 1, b), tweede zinsdeel van de algemene verordening gegevensbescherming: deze verwerkingen worden niet als onverenigbaar beschouwd met de oorspronkelijke doeleinden.

Artikel 2.1.2: Beoogde verwerking door [INSTANTIE 2] van Prioriteitsaanvragen

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

- Artikel 6.1.a, toestemming

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

- Het verlenen van een dienst voor het aanmaken en/of doorgeven van prioriteitsaanvragen voor specifieke weggebruikers, volgens een contractuele overeenkomst of volgens gebruiksvoorwaarden.
- 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

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

- Het verlenen van prioriteit aan specifieke weggebruikers op geconnecteerde kruispunten.
- Verdere verwerking: het aggregeren en daarna archiveren van de aanvragen voor het evalueren en verbeteren van de prioriteitsverlening.

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 prioriteitsverlening het doel van de oorspronkelijke verwerking is.

[EN]

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. De mededeling is evenwel toegelaten gezien het aanvragen van prioriteit een actieve vraag is, die zonder toestemming niet zal worden uitgestuurd.

[EN]

Het doeleinde voor de verdere verwerking is archivering in het algemeen belang en wetenschappelijk onderzoek. Op deze verwerkingen geldt een uitzondering volgens artikel 5, 1, b), tweede zinsdeel van de algemene verordening gegevensbescherming: deze verwerkingen worden niet als onverenigbaar beschouwd met de oorspronkelijke doeleinden.

Artikel 3: De gevraagde persoonsgegevens en de categorieën en omvang van de gevraagde persoonsgegevens conform het proportionaliteitsbeginsel

In onderstaande tabel wordt een overzicht gegeven van de verschillende persoonsgegevens die worden meegedeeld, 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 Weggebruikerposities- stroom [CAM en SRM0]	Weggebruikerposities-stroom [CAM en SRM0] bevat volgende persoonsgegevens: - Real-time verplaatsingsgegevens van geconnecteerde weggebruiker in de directe omgeving van geconnecteerde kruispunten in Vlaanderen - Type weggebruiker - Geplande beweging op het geconnecteerde kruispunt -
Verantwoording proportionaliteit	De verwerking van de gegevens is noodzakelijk om de regeling van de geconnecteerde kruispunten zo goed mogelijk af te stemmen op het werkelijke verkeer en indien mogelijk ook op de individueel geconnecteerde weggebruikers. De verwerking van de gegevens is noodzakelijk om de werking van de regelingen te kunnen evalueren en te verbeteren.
Gegeven 2 Prioriteitsaanvragen-stroom [SREMs, SSEMs en CAMs]	Prioriteitsaanvragen-stroom [SREMs, SSEMs en CAMs] bevat volgende persoonsgegevens: - Real-time verplaatsingsgegevens van weggebruikers waarvoor prioriteit wordt aangevraagd op een geconnecteerd kruispunt [CAMs] - Type en Rol van de betrokken weggebruikers - Konvooi-informatie van de betrokken weggebruikers - Aanvragen van prioriteit voor een beweging op het kruispunt met inschatting van aankomsttijd - Antwoorden op de aanvragen van prioriteit - 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 konvoien.
--	---

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 1 Weggebruikerposities-stroom [CAM en SRM0]	Voor de duur van de aanwezigheid op het kruispunt	Zolang de geconnecteerde weggebruiker in de buurt van het kruispunt is, blijven de gegevens relevant voor de optimalisatie van de verkeersstromen op het kruispunt.
Gegeven 2 Prioriteitsaanvragen-stroom [SREMs, SSEMs en CAMs]	6 maanden	6 maanden worden ingeschat als nodig voor het analyseren verbeteren en verzekeren van het goed verlenen van prioriteit op kruispunten.

De meegedeelde gegevens kan door [INSTANTIE 2] gedurende 3 maanden bewaard worden. Deze bewaartermijn kan worden verantwoord gezien de noodzaak voor het bijhouden voor de analyse en het verbeteren van de service.

Artikel 4: De categorieën van ontvangers en derden die mogelijks de gegevens eveneens verkrijgen

Artikel 4.2: Door [INSTANTIE 2]

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

Enkel personen van [INSTANTIE 2] die omwille van hun functieprofiel deze informatie nodig hebben voor de uitvoering van hun werk, krijgen toegang tot de informatie.

Elke eventuele 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 persoonsgegevens zullen continu worden uitgewisseld omdat het leveren van de diensten real-time gegevens vereist. De persoonsgegevens worden uitgewisseld tot uiterlijk 31/3/2025.

Artikel 6: Maatregelen voor verzekeren door [INSTANTIE 1] van geïnformeerde toestemming voor de verwerkingen van [INSTANTIE 2]

De toestemming voor de verwerkingen uit artikel 2.1.1 en 2.1.2 voldoet minimaal aan volgende voorwaarden:

- de betrokkene wordt voorafgaand aan het verkrijgen van de toestemming geïnformeerd over de doorgifte aan wegbeheerders en over de doeleinden van verwerking door wegbeheerders zoals vermeld in artikel 2.
- de informatie over de doorgifte en doeleinden blijft na het geven van toestemming raadpleegbaar
- indien geen toestemming gegeven is, of de toestemming werd gestopt, worden de gegevens van de betrokkene niet doorgestuurd. Dit wordt periodiek geverifieerd.
- de toestemming dient actief te worden gegeven (de optie staat standaard uit, m.a.w. opt-in)
- de toestemming kan worden gestopt aan de bron, waardoor nieuwe gegevens dan niet meer worden doorgegeven en nieuwe verwerkingen niet meer mogelijk zijn
- de toestemming voor de verwerkingen van wegbeheerders wordt afzonderlijk gegeven van andere doeleinden (bijvoorbeeld reclaimedoeleinden)
- indien de gegevens van een derde partij verkregen worden, worden deze voorwaarden aan deze derde partij contractueel opgelegd.

[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.

Artikel 7: Beveiligingsmaatregelen

Volgende maatregelen worden getroffen ter beveiliging van de mededeling van de persoonsgegevens, vermeld in artikel 2:

Artikel 7.1: 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 persoonsgegevens 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 persoonsgegevens 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 7.2: 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 gecentraliseerd en zijn doorzoekbaar

[INSTANTIE 2] treft ten minste volgende organisatorische en technische beveiligingsmaatregelen ter beveiliging van de ontvangen persoonsgegevens 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

Incident Response/Service Desk

- Een incident response team is ingesteld.
- Incident response policy en proces zijn vastgelegd.
- Een escalatieprocedure is vastgelegd. Bij zware incidenten wordt gerekend op een extern team.

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.
- Opleiding rond privacy bij on-boarding.
- Voor het uitsturen van persoonlijke gegevens kan gebeuren is een impact analyse verplicht.
- Verwerkingsovereenkomsten worden opgemaakt met derde partijen.
- Een procedure voor het afhandelen van subject requests is vastgelegd.

Fysieke Beveiliging

- Een inbraakalarm is aanwezig.
- Toegang gebeurt via een badgesysteem.
- Clear Desk & Screen 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

- Bij on-boarding wordt het belang van security en privacy benadrukt en wordt duidelijk gemaakt wat de verplichtingen zijn die bij de rol horen.
- Het arbeidscontract bevat een confidentiality en non-disclosure agreement.
- Tijdens de tewerkstelling wordt het belang van security en privacy benadrukt, bvb via trainingen.
- 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.
- Alle toegang wordt verwijderd binnen 24u na het ontslag van een werknemer.
- Een password policy is van kracht.
- Een penetratie test werd uitgevoerd.
- De autorisatie regels worden minstens per kwartaal 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.
- Monitoring is aanwezig, met een alerting systeem verbonden aan een wachtdienst.
- 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.
- Full Disk Encryption van werkstations en mobiele toestellen is verplicht.

[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 8: Kwaliteit van de persoonsgegevens

Zodra [INSTANTIE 1] of [INSTANTIE 2] één of meerdere foutieve, onnauwkeurige, onvolledige, ontbrekende, verouderde of overvloedige gegevens in de persoonsgegevens, 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 9: 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 persoonsgegevens 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 10: 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 11: 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 12: Inwerkingtreding en opzegging

Dit protocol treedt in werking op 01/06/2024.

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

Het protocol eindigt van rechtswege na afloop van de in artikel 5 van dit protocol bedoelde termijn van mededeling. Het protocol eindigt tevens van rechtswege wanneer er geen rechtsgrond meer bestaat voor de gevraagde doorgifte van persoonsgegevens.

Artikel 13: Ondertekening van het protocol

Partijen komen overeen dat:

- een elektronische handtekening in de zin van een geavanceerde of gekwalificeerde elektronische handtekening overeenkomstig de Europese eIDAS Verordening nr. 910/2014 of
- gescande kopieën van de handgetekende overeenkomst in elektronisch formaat,

dezelfde wettelijke bewijskracht bezitten als een handgetekend origineel document.

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

Gelieve er rekening mee te houden dat in de onderliggende gegevens van de digitale handtekening uw rijksregisternummer zichtbaar is. Door uw digitale handtekening te plaatsen verklaart u zich akkoord dat uw rijksregisternummer kenbaar is voor de ontvanger van het document.

