Overeenkomst voor de verwerking van persoonsgegevens

TUSSEN **Stad Gent**, met zetel ten Stadhuize, te 9000 Gent, Botermarkt 1, vertegenwoordigd door het college van burgemeester en schepenen, voor wie tekenen, de heer Mathias De Clercq, burgemeester, en mevrouw Mieke Hullebroeck, algemeen directeur.
In uitvoering van het collegebesluit d.d. _____

hierna "de *Verwerkingsverantwoordelijke*" genoemd, enerzijds

EN **SWARCO Belgium NV,** naamloze vennootschap, met zetel te Paapsemlaan 20 te 1070 Anderlecht België, vertegenwoordigd door de heer Danny Asselman, Managing Director

hierna "de *Verwerker"* genoemd, anderzijds,

samen "de *Partijen*" of afzonderlijk "*Partij*" te noemen

wordt

TEN BEHOEVE VAN DE OVEREENKOMST

Uitrol van i-VRI's voor de stad Gent binnen de raamovereenkomst VWT/INN/2022/9 – Mobilidata – i-VRI – leveren, opstellen, onderhouden en aanpassen van intelligente verkeersregelaars in Vlaanderen – gedeelte ITS-Applicatie en RIS 3

begindatum: 15 november 2024 looptijd: 8 jaar per indienstname kruispunt

hierna "de *Opdracht*" te noemen.

overeengekomen wat volgt:

Artikel 1. Definities

Persoonsgegevens zijn, zoals vermeld in artikel 4.1 van de *Algemene Verordening Gegevens-bescherming*[1] (hierna AVG te noemen): "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*";

De *Verwerkingsverantwoordelijke* is, zoals vermeld in artikel 4.7 van de AVG, "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen*".

De *Verwerker* is, zoals vermeld in artikel 4.8 van de AVG, "*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerkings-verantwoordelijke persoonsgegevens verwerkt*".

De in deze overeenkomst bedoelde *Verwerkingen* zijn verwerkingen in de zin van artikel 4.2 van de AVG: "*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*".

Artikel 2. Voorwerp van de overeenkomst

De *Verwerkingsverantwoordelijke* bezorgt aan de *Verwerker* de persoonsgegevens genoemd in Bijlage 1 bij deze overeenkomst (hierna de "*Gegevens*" te noemen). Voor de volledige duur van deze overeenkomst onderwerpt de *Verwerker* de *Gegevens* aan de verwerkingen vermeld in Bijlage 1, volgens de voorwaarden die in deze overeenkomst worden gesteld.

Artikel 3. Duur van de overeenkomst

De duur van deze overeenkomst is gelijk aan de duur van de *Opdracht*, onverlet de bepalingen van artikel 9 van deze overeenkomst ("Einde van de overeenkomst").

Artikel 4. Verwerking

§ 1. De *Verwerker* en al wie onder zijn verantwoordelijkheid of gezag handelt en toegang heeft tot de *Gegevens*, verwerkt de *Gegevens* uitsluitend volgens de schriftelijke instructies van de *Verwerkings-verantwoordelijke* in het kader van de in Bijlage 1 beschreven doelen. De *Verwerker* treft maatregelen om dit te waarborgen.

[1] VERORDENING (EU) 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 (algemene verordening gegevensbescherming) (http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL).

§ 2. Het eerste lid is niet van toepassing wanneer een op de *Verwerker* van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de *Verwerker* de *Verwerkingsverantwoordelijke*, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

§ 3. Gegevens die, in het kader van de *Opdracht* die door meerdere partijen waaronder de *Verwerker* wordt uitgevoerd, door de *Verwerker* moeten worden meegedeeld aan één of meer der andere partijen, mogen alleen na een schriftelijke toestemming van de *Verwerkingsverantwoordelijke* daartoe, aan die andere partij(en) worden meegedeeld.

Artikel 5. Verbintenissen van de Partijen

§ 1. De partijen verbinden zich er toe om alle huidige en toekomstige op de verwerking van persoonsgegevens van toepassing zijnde wet- en regelgeving na te leven.

§ 2. Alleen de persoonsgegevens die strikt noodzakelijk zijn voor de uitvoering van de *Opdracht* mogen door de *Verwerker* worden verwerkt. De *Verwerkingsverantwoordelijke* stelt de persoonsgegevens onverwijld ter beschikking van de *Verwerker* voor de verwerking ervan in het kader van de *Opdracht*.

§ 3. De *Verwerker* verbindt zich tot:

I. de verzekering dat de *Verwerking* van de persoonsgegevens gebeurt onder het toezicht van een eigen functionaris voor gegevensbescherming als bedoeld in artikel 37 tot en met 39 van de AVG;

II. de beschikbaarheid van een eigen informatieveiligheidsbeleid;

III. het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkenen zijn gewaarborgd.

De bestanden met de Gegevens mogen in geen geval vrij toegankelijk zijn, maar moeten worden beschermd met toegangscodes en wachtwoorden die regelmatig worden vernieuwd door de Verwerker.

Rekening houdend 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, treft de *Verwerker* passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Waar passend dienen deze maatregelen onder meer te omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de *verwerkingsrisico's*, vooral als gevolg van de *vernietiging*, het *verlies*, de *wijziging* of de *ongeoorloofde verstrekking* van of *ongeoorloofde toegang* tot doorgezonden, opgeslagen of anderszins verwerkte *Gegevens*, hetzij per ongeluk hetzij onrechtmatig.

Onder voorbehoud van uitzonderingen die het zakengeheim rechtvaardigen, geeft de *Verwerker* de *Verwerkingsverantwoordelijke* kennis van alle veiligheidsmaatregelen die hij neemt om de wettelijke bepalingen na te komen.

IV. de beschikbaarheid van een eigen informatieveiligheidsplan dat in de concrete uitwerking van de verschillende voornoemde maatregelen voorziet;

V. het treffen van de volgende maatregelen:

a) het aanwijzen van de personen die de persoonsgegevens kunnen verwerken, waarbij hun hoedanigheid ten opzichte van de verwerking van de *Gegevens* nauwkeurig moet worden omschreven; de *Verwerker* garandeert, dat deze personen uitsluitend toegang hebben tot de *Gegevens* die ze nodig hebben om hun taak of opdracht in het kader van deze overeenkomst uit te voeren;

b) ervoor te zorgen dat de aangewezen personen, vermeld in punt (a), door een wettelijke of statutaire verplichting, of door een evenwaardige contactuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken *Gegevens* in acht te nemen. Op eenvoudige vraag deelt de *Verwerker* de *Verwerkingsverant-woordelijke* schriftelijk mee op welk van de genoemde wijzen de vertrouwelijkheid gewaarborgd is en bezorgt de *Verwerkingsverantwoordelijke* een afschrift van de relevante documenten (bv. vertrouwelijkheidsclausule uit het Arbeidsreglement);

c) de personen, vermeld in punt (a), kennis te geven van de bepalingen van de onder artikel 5 §1 vermelde wetgeving en normering, en van elk ander van toepassing zijnde voorschrift betreffende de bescherming van persoonsgegevens. Op eenvoudige vraag deelt de *Verwerker* aan de *Verwerkingsverantwoordelijke* schriftelijk mee hoe de bedoelde kennisgeving gebeurd is en bezorgt de *Verwerkings-verantwoordelijke* een afschrift van de relevante documenten;

§ 4. De *Verwerker* verbindt zich ertoe de noodzakelijke software en uitrustingen te verwerven, te onderhouden en regelmatig bij te werken – evenals de licenties die vereist zijn voor hun wettelijk gebruik – opdat hij beschikt over een systeem dat conform is aan de laatste stand van de techniek teneinde zijn verbintenissen krachtens deze overeenkomst na te komen.

§ 5. De *Verwerker* verleent aan de *Verwerkingsverantwoordelijke* door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand bij het vervullen van diens plicht om verzoeken tot uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene, te beantwoorden.

§ 6. Rekening houdend met de aard van de verwerking en de aan de *Verwerker* ter beschikking staande informatie, verleent de *Verwerker* de *Verwerkingsverantwoordelijke* bijstand bij het nakomen van diens verplichtingen betreffende:

I. het beveiligen van de verwerking conform artikel 32 van de AVG;

II. het melden van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit conform artikel 33 van de AVG;

III. het mededelen van een inbreuk in verband met persoonsgegevens aan de betrokkene conform artikel 34 van de AVG;

IV. het uitvoeren van een Gegevensbeschermingseffectbeoordeling conform artikel 35 van de AVG;

V. het voorafgaand aan een voorgenomen verwerking raadplegen van de toezichthoudende autoriteit, wanneer dit na een Gegevensbeschermings-effectbeoordeling nodig zou blijken, conform artikel. 36 van de AVG.

§ 7. De *Verwerker* informeert de *Verwerkingsverantwoordelijke* zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. De *Verwerker* verstrekt de *Verwerkingsverantwoordelijke* op diens verzoek alle informatie betreffende de inbreuk.

§ 8. De *Verwerker* stelt de *Verwerkingsverantwoordelijke* alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen van de *Verwerker* ingevolge deze overeenkomst aan te tonen. De *Verwerker* maakt audits, waaronder inspecties, door de *Verwerkingsverantwoordelijke* of een door de *Verwerkingsverantwoordelijke* gemachtigde controleur mogelijk en draagt eraan bij. In dit verband stelt de *Verwerker* de *Verwerkingsverantwoordelijke* onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op de AVG of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming

§ 9. Het is de *Verwerker* toegelaten om in het kader van de *Opdracht* een kopie van de *Gegevens* te maken als dit noodzakelijk is voor het uitvoeren van de *Opdracht*. De *Verwerker* kan ook overgaan tot het nemen van een back-up. Voor het gebruik van kopieën en back-ups gelden dezelfde regels als voor het gebruik van de originele *Gegevens*.

§ 10. De *Verwerker* bezorgt de *Verwerkingsverantwoordelijke*, telkens wanneer die erom verzoekt, een kopie van de *Gegevens* die in het kader van deze overeenkomst worden verwerkt in een onderling te bepalen formaat.

§ 11. De *Verwerker* verbindt zich ertoe niet te handelen, en zal ook niemand toelaten te handelen, op een manier die strijdig is met de verbintenissen die in deze overeenkomst worden bepaald of met de wettelijke verbintenissen die van toepassing zijn;

Artikel 6. Onderaanneming

§ 1. Dit zijn de Subverwerkers zoals deze aan het begin van de opdracht gekend zijn:

- SWARCO Peek Traffic B.V. uit Nederland voor levering van diensten met betrekking om een ITS-applicatie en RIS functioneel te laten werken, waarbij beide applicaties volgens het Software as a Service-principe worden afgenomen van de categorie Indentificatiegegevens.
- SWARCO Nederland B.V. uit Nederland voor levering van diensten met betrekking om een RIS functioneel te laten werken, waarbij beide applicaties volgens het Software as a Service-principe worden afgenomen van de categorie Indentificatiegegevens.

§ 2. De *Verwerker* neemt geen andere verwerker ("onderaannemer", "subverwerker") in dienst zonder voorafgaande algemene schriftelijke toestemming van de *Verwerkingsverantwoordelijke*. Wanneer deze toestemming gegeven is, licht de *Verwerker* de *Verwerkingsverantwoordelijke* in over alle beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de *Verwerkingsverantwoordelijke* de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken;

§ 3. Wanneer een *Verwerker* een andere verwerker in dienst neemt om voor rekening van de *Verwerkingsverantwoordelijke* specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de voorliggende overeenkomst tussen de *Verwerkingsverantwoordelijke* en de *Verwerker* zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in de voorliggende overeenkomst en de AVG voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de (eerste) *Verwerker* ten aanzien van de *Verwerkingsverantwoordelijke* volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

Artikel 7. Verantwoordelijkheden en waarborgen

§ 1. De *Verwerkingsverantwoordelijke* verzekert dat alle *Gegevens* die hij in het kader van deze overeenkomst aan de *Verwerker* bezorgt wettelijk aan de *Verwerker* mogen worden meegedeeld conform de wetgeving (waaronder begrepen de AVG).

§ 2. De *Verwerker* waarborgt, voor zover dit technisch mogelijk is, de integriteit, de beschikbaarheid en het bijwerken van alle *Gegevens* die hij in het kader van deze overeenkomst verwerkt.

§ 3. De *Verwerker* verzekert dat geen enkele uitrusting of software die hij in het kader van deze overeenkomst gebruikt een inbreuk uitmaakt op het intellectuele eigendomsrecht van een derde (zoals het auteursrecht, octrooi, recht *sui generis*, merk, …).

§ 4. De *Verwerker* is aansprakelijk voor de veiligheid en het goede gebruik van de toegangscodes, gebruikersnamen en wachtwoorden, alsook voor het regelmatig wijzigen van deze codes en wachtwoorden, om toegang te hebben tot de *Gegevens* en ze te verwerken. De *Verwerker* verbindt zich ertoe alles in het werk te stellen opdat al wie toegang heeft tot de *Gegevens* de vertrouwelijkheid van zijn codes en wachtwoorden zou bewaren. Hij verbindt zich ertoe de *Verwerkingsverantwoordelijke* op de hoogte te stellen van elk veiligheidsincident en van de acties die hij onderneemt om de incidenten te verhelpen.

§ 5. De *Verwerker* vrijwaart de *Verwerkingsverantwoordelijke* tegen elke klacht die een derde indient, inclusief de bevoegde toezichthoudende autoriteit, op grond van de AVG en andere op de verwerking van persoonsgegevens van toepassing zijnde wet- en regelgeving, en die het gevolg zou zijn van een handeling of een nalatigheid van de *Verwerker* in strijd met zijn verbintenissen in overeenstemming

met deze overeenkomst of met de AVG en andere op de verwerking van persoonsgegevens van toepassing zijnde wet- en regelgeving.

§ 6. Wanneer de *Verwerker* ISO 2700x gecertificeerd is, mag dit certificaat bij deze overeenkomst gevoegd worden. Het certificaat moet gezien worden als pluspunt ten opzichte van verwerkers die niet gecertificeerd zijn en het kan niet in de plaats van deze overeenkomst, of delen daarvan, gesteld worden.

Artikel 8. Intellectuele eigendom

Alle rechten van intellectuele eigendom op de *Gegevens* en op de databases met deze *Gegevens* behoren toe aan de *Verwerkingsverantwoordelijke*, tenzij dit contractueel anders overeengekomen wordt tussen de Partijen.

Artikel 9. Einde van de overeenkomst

Deze overeenkomst eindigt wanneer de overeenkomst voor de uitvoering van de *Opdracht*, vermeld in deze overeenkomst, een einde neemt.

Wanneer deze verwerkersovereenkomst een einde neemt, bezorgt de *Verwerker* aan de *Verwerkingsverantwoordelijke* of aan al wie de *Verwerkingsverantwoordelijke* aanstelt een actuele kopie van de *Gegevens* en van de databases met de gegevens die het resultaat zijn van de verwerking waarmee de *Verwerker* werd belast. Hij bezorgt de *Verwerkingsverantwoordelijke* ook gelijk welke informatie of documenten die nodig zijn voor de latere verwerking van de *Gegevens*. Voorgaande overdrachten gebeuren zonder extra kosten en op een wijze die de *Verwerkingsverantwoordelijke* bepaalt. De *Verwerker* zal zorgen dat alle *Gegevens* en databases in het formaat dat door de *Verwerkingsverantwoordelijke* wordt bepaald, worden doorgegeven naar het informaticasysteem dat door de *Verwerkingsverantwoordelijke* wordt aangewezen.

Als alle *Gegevens* en databases zijn doorgegeven, stelt de *Verwerker* onmiddellijk een einde aan elke verwerking van de *Gegevens* en vernietigt hij elke kopie en back-up (zie punt 5.j) van de *Gegevens* en databases die hij nog zou bezitten zonder extra kosten voor de *Verwerkingsverantwoordelijke* en op een wijze die de *Verwerkingsverantwoordelijke* bepaalt, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

De vertrouwelijkheidsverbintenissen die door deze overeenkomst ontstaan, duren voort na het verstrijken van deze overeenkomst.

Artikel 10. Volledigheid van de overeenkomst

Indien gelijk welk beding van deze overeenkomst wordt vernietigd of op eender welke andere wijze ongeldig wordt verklaard, blijft de rest van de overeenkomst bestaan en wordt het bewuste beding vervangen door een geldig beding dat zo goed mogelijk de initiële bedoeling van de Partijen weergeeft.

Artikel 11. Toepasselijk recht en betwisting

In geval van betwisting is het Belgische recht van toepassing en zijn de hoven en rechtbanken van het gerechtelijk arrondissement Oost-Vlaanderen, afdeling Gent bevoegd.

Opgemaakt te Anderlecht waarbij elke partij verklaart deze overeenkomst ontvangen en goedgekeurd te hebben.

Voor de *Verwerkingsverantwoordelijke*,
Stad Gent,

Mieke Hullebroeck
Algemeen Directeur

Mathias De Clercq
Burgemeester

Voor de verwerker,

Danny Asselman
Bestuurder SWARCO Belgium

Gerrit Van den Heuvel
Bestuurder SWARCO Belgium

BIJLAGE 1 bij de overeenkomst voor de verwerking van persoonsgegevens

In het kader van de overeenkomst voor de verwerking van persoonsgegevens, voert de *Verwerker* op de onderstaande persoonsgegevens de verwerkingen uit waarvan per gegevenssoort de aard van de verwerking, alsmede het doel ervan en de categorieën van betrokkenen worden vermeld.

Omschrijving van de verwerking	Doeleinde van de verwerking	Soort persoonsgegeven(s)	Categorie(ën) van betrokkenen
Persoonsgegevens raadplegen Het gaat om diensten van de Verwerker waarbij de persoonsgegevens van de Verwerkingsverantwoordelijke bekeken kunnen worden door medewerkers of Onderaannemers van de Verwerker, waaronder maar niet beperkt tot, servicedesk Diensten, (remote) monitoring Diensten, system management Diensten, technisch applicatie management, vulnerability scanning Diensten, rapporting Diensten in governance en software asset management Diensten	• Optimalisatie en verbeteren van verkeersregelingen • Verlenen van prioriteit aan specifieke doelgroepen	• Identificatiegegevens en Logging-gegevens van de medewerkers van de Verwerkingsverantwoordelijke bij het gebruik van de diensten en bijhorende producten van de *Verwerker* • pseudo-anonieme locatie- en verplaatsingsgegevens • pseudo-anonieme voertuigtype- of weggebruikertype-gegevens • pseudo-anonieme snelheden en/of versnellingen • pseudo-anonieme prioriteitsaanvragen	• Burgers, werknemers van hulpdiensten en bedrijven • medewerkers van de Verwerkingsverantwoordelijke • medewerkers van AWV verantwoordelijk voor de goede werking van het Mobilidata-ecosysteem. • Aannemers die voor de goede werking van de (i)-VRI's indienste staan van de Verwerkingsverantwoordelijke
Persoonsgegevens opslag Het gaat om diensten van de Verwerker waarbij de persoonsgegevens van de Verwerkingsverantwoordelijke opgeslagen worden in een door de Verwerker geleverd opslagsysteem zoals onder meer maar niet beperkt tot cloud storage Diensten, cloud backup Diensten, file Diensten, directory Diensten, managed file transfer, mail & calendaring and logfile processing.	• Optimalisatie en verbeteren van verkeersregelingen • Verlenen van prioriteit aan specifieke doelgroepen	• Identificatiegegevens en Logging-gegevens van de medewerkers van de Verwerkingsverantwoordelijke bij het gebruik van de diensten en bijhorende producten van de *Verwerker* • pseudo-anonieme locatie- en verplaatsingsgegevens • pseudo-anonieme voertuigtype- of weggebruikertype-gegevens • pseudo-anonieme snelheden en/of versnellingen • pseudo-anonieme prioriteitsaanvragen	• Burgers, werknemers van hulpdiensten en bedrijven • medewerkers van de Verwerkingsverantwoordelijke • medewerkers van AWV verantwoordelijk voor de goede werking van het Mobilidata-ecosysteem. • Aannemers die voor de goede werking van de (i)-VRI's indienste staan van de Verwerkingsverantwoordelijke

<u>Persoonsgegevens doorzenden</u> Het betreft diensten van de Verwerker waarbij persoonsgegevens van de Verwerkingsverantwoordelijke verzonden worden van, naar of tussen applicaties op een door de Verwerker beheerd platform zoals onder meer maar niet beperkt tot LAN Diensten, Wide Area Network Diensten, data center interconnectiviteitsdiensten, Loadbalancing, SAN switch interconnects en Diensten die geleverd worden over de Voice over Internet Protocol (VoIP).	• Optimalisatie en verbeteren van verkeersregelingen • Verlenen van prioriteit aan specifieke doelgroepen	• Identificatiegegevens en Logging-gegevens van de medewerkers van de Verwerkingsverantwoordelijke bij het gebruik van de diensten en bijhorende producten van de *Verwerker* • pseudo-anonieme locatie- en verplaatsingsgegevens • pseudo-anonieme voertuigtype- of weggebruikertype-gegevens • pseudo-anonieme snelheden en/of versnellingen • pseudo-anonieme prioriteitsaanvragen	• Burgers, werknemers van hulpdiensten en bedrijven • medewerkers van de Verwerkingsverantwoordelijke • medewerkers van AWV verantwoordelijk voor de goede werking van het Mobilidata-ecosysteem. • Aannemers die voor de goede werking van de (i)-VRI's indienste staan van de Verwerkingsverantwoordelijke
<u>Persoonsgegevens bijwerken of wijzigen</u> Het betreft diensten van de Verwerker waarbij persoonsgegevens van de Verwerkingsverantwoordelijke aangepast kunnen worden zowel op manuele, als op geautomatiseerde wijze zoals bij een geautomatiseerde job flow die ondersteund wordt door een job scheduling system.	• Optimalisatie en verbeteren van verkeersregelingen • Verlenen van prioriteit aan specifieke doelgroepen	• Identificatiegegevens en Logging-gegevens van de medewerkers van de Verwerkingsverantwoordelijke bij het gebruik van de diensten en bijhorende producten van de *Verwerker* • pseudo-anonieme locatie- en verplaatsingsgegevens • pseudo-anonieme voertuigtype- of weggebruikertype-gegevens • pseudo-anonieme snelheden en/of versnellingen • pseudo-anonieme prioriteitsaanvragen	• Burgers, werknemers van hulpdiensten en bedrijven • medewerkers van de Verwerkingsverantwoordelijke • medewerkers van AWV verantwoordelijk voor de goede werking van het Mobilidata-ecosysteem. • Aannemers die voor de goede werking van de (i)-VRI's indienste staan van de Verwerkingsverantwoordelijke

<u>Software testen</u> Het gaat om diensten van de Verwerker waarbij databanken van de Verwerkingsverantwoordelijke die persoonsgegevens bevatten (persoonsgegevens die niet geanonimiseerd zijn), worden gebruikt buiten de productie omgeving (in test, acceptatie,…) als onderdeel van het testproces van de software applicatie.	• Optimalisatie en verbeteren van verkeersregelingen • Verlenen van prioriteit aan specifieke doelgroepen	• Identificatiegegevens en Logging-gegevens van de medewerkers van de Verwerkingsverantwoordelijke bij het gebruik van de diensten en bijhorende producten van de *Verwerker* • pseudo-anonieme locatie- en verplaatsingsgegevens • pseudo-anonieme voertuigtype- of weggebruikertype-gegevens • pseudo-anonieme snelheden en/of versnellingen • pseudo-anonieme prioriteitsaanvragen	• Burgers, werknemers van hulpdiensten en bedrijven • medewerkers van de Verwerkingsverantwoordelijke • medewerkers van AWV verantwoordelijk voor de goede werking van het Mobilidata-ecosysteem. • Aannemers die voor de goede werking van de (i)-VRI's indienste staan van de Verwerkingsverantwoordelijke

BIJLAGE 2 - Technische en Organisatorische maatregelen in het kader van de AVG

1. Van toepassing zijnde regelgeving

i. de AVG;
ii. de Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018 (Kaderwet aka nieuwe privacywet)[2]
iii. het Decreet van 8 juni 2018 houdende de aanpassing van de decreten aan de verordening (EU) 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 (algemene verordening gegevensbescherming) aka het AVG-Decreet2;
iv. de *Minimale normen informatieveiligheid en privacy*[3] voor sociale zekerheidsinstellingen die toegang willen bekomen en behouden tot het netwerk van de Kruispuntbank;
v. de bepalingen van de *Wet tot regeling van een Rijksregister van de natuurlijke personen* van 8 augustus 1983.[4]
vi. De adviezen van de Vlaamse Toezichtscommissie

2. Bepalingen art 32 AVG

Rekening houdend 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, treffen de *Verwerkingsverantwoordelijke* en de *Verwerker* passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. De *Verwerker* is eraan gehouden om maatregelen te treffen die onder meer het volgende omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de Verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking

3. Technische en organisatorische maatregelen betreffende het platform waar de Verwerkingsverantwoordelijke mee werkt

Onderstaande lijst is op te vatten als een afchecklijst. Gevraagd wordt dat de *Verwerker* aangeeft in de tweede kolom – door aan te vinken - of deze maatregelen al dan niet worden genomen.
Indien in de derde kolom de maatregel als verplicht wordt aangegeven en de maatregel is niet aanwezig, dient de Verwerker in de vierde kolom de reden hiervoor te verantwoorden.

---

[2] https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Wet_Loi_30_07_2018.pdf

[3] https://www.ksz-bcss.fgov.be/sites/default/files/assets/veiligheid_en_privacy/mnm_minimale_normen_v2017.pdf

[4] http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl?language=nl&caller=list&cn=1983080836&la=n&fromtab=wet&sql=dt=%27wet%27&tri=dd+as+rank&rech=1&numero=1

Maatregel	Aanwezig	Verplicht	Verantwoording
De aanwezigheid van automatische anonimisering of pseudonimisering van de persoonsgegevens nadat het doeleinde van de verwerking (of wettelijke opgelegde bewaartermijnen) zijn overschreden		√	
De aanwezigheid van een degelijk uitgebouwd gebruikersbeheer		√	
De aanwezigheid van een degelijk uitgebouwde audit log module		√	
Mogelijkheid tot extractie (export) van gegevens / back-up mogelijkheid		√	
De webapplicatie is uitgerust met een bescherming tegen een brute force aanval. Na X keer foutief inloggen wordt de gebruiker geblokkeerd.		√	
Persoonsgegevens worden aan de *Verwerkingsverantwoordelijke* ter beschikking gesteld via een beveiligde verbinding (https, VPN, IPSEC, FTPs)		√	
Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de Verwerkingssystemen en diensten te garanderen;		√	
Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;		√	
Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.		√	

4. <u>Technische en organisatorische maatregelen betreffende de interne werking en organisatie van SWARCO Belgium NV.</u>

Onderstaande lijst is op te vatten als een afchecklijst. Gevraagd wordt dat de *Verwerker* aangeeft in de tweede kolom of deze maatregelen al dan niet worden genomen.

	Aa

Maatregel	nwezig	Verplicht	Verantwoording
ALGEMEEN BEVEILIGINGSBELEID EN ORGANISATIE VAN INFORMATIEBEVEILIGING			
Verantwoordelijke voor informatiebeveiliging: SWARCO Belgium heeft informatieveiligheidsconsulent aangesteld die verantwoordelijk is voor de data beveiliging ⇨ contactgegevens:gerrit.van.den.heuvel@swarco.com		√	√
Verantwoordelijke voor gegevensbescherming: SWARCO Belgium heeft een Data Pr otection Officer aangewezen die verantwoordelijk is voor het coördineren, opvolgen en controleren van de beveiligingsregels en -procedures. ⇨ Contactgegevens: sbe-gdpr@swarco.com		√	√
Informatieveiligheidsbeleid: SWARCO Belgium beschikt over een goedgekeurd informatieveiligheidsbeleid.		√	√
Informatieveiligheidsplan: SWARCO Belgium beschikt over een eigen informatieveiligheidsplan dat in de concrete uitwerking van de verschillende voornoemde maatregelen voorziet;		√	√
Verantwoordelijkheden op vlak van informatiebeveiliging en gegevensbescherming: De verantwoordelijkheden van de medewerkers van SWARCO Belgium zijn formeel gedocumenteerd en gepubliceerd in een privacy- en security policy.		√	√
Risico analyse, beheer en controle: SWARCO Belgium voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende informatiebeveiligingsprocedures		√	√

VEILIG PERSONEELSBELEID			
Training over belang van beveiliging en omgang met persoonsgegevens: SWARCO Belgium voorziet opleidingen om alle medewerkers te sensibiliseren voor wat betreft de beveiligingsrichtlijnen- en beveiligingsprocedures en hun rol daarbij.		√	√
Aanduiding personeel: SWARCO Belgium wijst aan de personen die de persoonsgegevens kunnen verwerken, waarbij hun hoedanigheid ten opzichte van de verwerking van de persoonsgegevens nauwkeurig worden omschreven.		√	√

[Naam Verwerker] garandeert dat deze personen uitsluitend toegang hebben tot de Gegevens die ze nodig hebben om hun taak of opdracht in het kader van deze Verwerkersovereenkomst uit te voeren.			
Lijst personeel: SWARCO Belgium houdt de lijst van personen, vermeld in in het vorige punt ter beschikking van de Gegevensbeschermingsautoriteit;		√	√
Verplichting tot vertrouwelijkheid: SWARCO Belgium zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contactuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken Gegevens in acht te nemen. SWARCO Belgium deelt de Verwerkingsverantwoordelijke schriftelijk mee op welk van de genoemde wijzen de vertrouwelijkheid gewaarborgd is. Een mogelijk voorbeeld van een vertrouwelijkheidscontract is terug te vinden in Bijlage 6.		√	√
Toegangsautorisatie: SWARCO Belgium implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die persoonsgegevens bevatten. SWARCO Belgium staat in voor de veiligheid en het goede gebruik van de toegangscodes, gebruikersnamen en wachtwoorden, alsook voor het regelmatig wijzigen van deze codes en wachtwoorden, om toegang te hebben tot de persoonsgegevens.		√	√
Segregatie: SWARCO Belgium heeft een segregatie ingevoerd om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak.		√	√

FYSIEKE BEVEILIGING			
Fysieke toegang tot productie- en bureauruimtes: SWARCO Belgium beperkt de toegang tot haar ruimtes waar persoonsgegevens verwerkt worden in kader van haar opdracht, strikt tot geïdentificeerde en geautoriseerde personen. Hiervoor werden badge-lezers geïnstalleerd, werd de lift uitgerust met codes en werden sloten voorzien op deuren waar nog nodig, dit alles om ongeoorloofde toegang te vermijden.		√	Lift voorzien met codes is niet nodig.
Beveiliging van de omgeving: Naast badge-lezers is het volledige gebouw uitgerust met - camerabewaking - een alarm- en branddetectie systeem.		√	√
Fysieke toegang tot het Data Center: SWARCO Belgium centraliseerde alle data die nodig is in kader van haar opdracht in een beveiligd data center		√	√

conform de industrienormen. Fysieke toegang tot het data center wordt gecontroleerd / beheerd.			
Noodherstel: SWARCO Belgium beschikt over een noodherstelplan in geval van calamiteiten met haar servers in het Data Center waarop persoonsgegevens staan		√	√
Redundantie: SWARCO Belgium bewaart kopieën van persoonsgegevens alsook haar gegevensherstelprocedures welke opgeslagen staan in het primaire data center in een tweede data center. => Deze kopieën zijn extra versleuteld met specifieke encryptie sleutels die enkel nodig zijn indien het primaire data center zou falen.		√	√

BESCHERMING TEGEN ONGEREGELDHEDEN, PANNES EN INCIDENTEN			
Firewall: SWARCO Belgium is uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang tot zijn interne netwerk.		√	√
Monitoring: SWARCO Belgium monitort en beheert het netwerk en de informatiesystemen op een actieve wijze. SWARCO Belgium beschikt over een procedure op om een eventuele inbreuk af te handelen, met inbegrip van informatie aan de Verwerkingsverantwoordelijke.		√	√

DIGITALE GEGEVENS			
Versleuteling van gegevens: alle digitale gegevens die verwerkt worden door SWARCO Belgium in kader van haar opdracht worden centraal in het data center op een versleutelde manier bewaard op de harde schijven		√	√
Anti-virus en beveiligingsupdates: SWARCO Belgium voorziet al zijn systemen van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens haar patchmanagementproces		√	√
Kwaadaardige Software: SWARCO Belgium voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantengegevens krijgt.		√	√
Logging van toegangen. SWARCO Belgium voorziet een continue logging op de server van alle toegangen tot haar systemen die persoonsgegevens bevatten met inbegrip van welke gebruiker, de tijd en activiteit. Alle logbestanden worden gedurende 90 dagen bijgehouden.		√	√

BEVEILIGDE VERBINDINGEN			
Versleuteling van verbindingen: SWARCO Belgium maakt gebruikt van beveiligde verbindingen voor de toegang tot haar gegevens in het		√	√

datacenter. Alle data die verzonden wordt over publieke netwerken gebeurt dan ook aan de hand van encryptie mechanismen. ⇨ https ⇨ VPN			

AUTHENTICATIE			
Two-factor authenticatie: SWARCO Belgium maakt gebruik van een combinatie van gebruikers/wachtwoord en een dynamisch token waarvan de geldigheid iedere 30 second vervalt. Wachtwoorden dienen steeds te bestaan uit minimaal acht tekens en zowel uit minimaal één hoofdletter, letter, cijfer.		√	√ Enkel van toepassing voor toegang tot systemen met persoonsgegevens en netwerk van klanten.

ONDERHOUD EN EVOLUTIE VAN INFORMATIESYSTEMEN			
Controle over systeem updates en evoluties: SWARCO Belgium heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.		√	√
Beveiligingsvereisten: De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd in samenwerking met onze IT leverancier(s).		√	√

INCIDENTEN			
Incident response: SWARCO Belgium houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld.		√	√
Notificatie van incidenten: In geval van een gegevensbeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van persoonsgegevens van klanten, zal SWARCO Belgium, zonder onredelijke vertraging, de *Verwerkingsverantwoordelijke* hiervan informeren.		√	√