

**PROTOCOL VOOR DE ELEKTRONISCHE MEDEDELING VAN PERSOONSgegevens TUSSEN
AGENTSCHAP WEGEN EN VERKEER EN JdSoft**

in het kader van [MOBILIDATA TOEPASSINGEN VOOR HULPDIENTEN]

[29/8/2025]

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

TUSSEN

Het VLAAMSE GEWEST,

in deze vertegenwoordigd door de Vlaamse regering, bij delegatie in hoofde van mevr. Annick De Ridder, Vlaams minister voor Mobiliteit, Openbare Werken, Havens en Sport,

in deze bij delegatie vertegenwoordigd door mevr. ir. Kathy Vandenmeersschaut, in haar hoedanigheid van administrateur-generaal van het intern verzelfstandigd zonder rechtspersoonlijkheid

Agentschap Wegen en Verkeer,

entiteit ingeschreven in de Kruispuntbank Ondernemingen onder het ondernemingsnummer 0316.380.841 met vestigingseenheid te 1000 BRUSSEL, Simon Bolivarlaan 17 bus 420

hierna: “**AWV**”;

EN

JdSoft B.V., vertegenwoordigd door Jan Van Hooydonck, Bestuurder/CEO,

ingeschreven in het KBO met nummer BE0460.831.756, waarvan de administratieve zetel zich bevindt te Vaartstraat 17, 2960 Brecht

hierna: “**Service Provider**”;

[AWV] en [Service Provider] worden hieronder ook wel afzonderlijk aangeduid als een “partij” of gezamenlijk als de “partijen”;

NA TE HEBBEN UITEENGEZET

- A. [AWV] 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 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. [Service Provider], JD SOFT BV, is een softwarebedrijf gespecialiseerd in het verwerken van dringende interventies via de noodcentrales 112 voor spoeddiensten en Ziekenwagendiensten. (MUG | Ziekenwagen | PIT). Haar visie: het verbeteren van de veiligheid, efficiëntie en samenwerking bij noodsituaties door innovatieve oplossingen te bieden in een gebruiksvriendelijk en platform-onafhankelijke oplossing. Een wereld waarin hulpdiensten, first-responders en organisaties moeiteloos samenwerken om levens te redden, schade te beperken of te voorkomen
- C. Mobilidata is een programma van de Vlaamse overheid waarin overheden, bedrijven en onderzoekers samenwerken om innovatieve technologische verkeersoplossingen te ontwikkelen en te implementeren. Het doel is om het verkeer veiliger, vlotter, duurzamer en comfortabeler te maken voor alle weggebruikers. Dit wordt bereikt door het gebruik van intelligente data en technologieën zoals intelligente verkeerslichten, verbeterde routeadviezen en op maat gemaakte verkeersmeldingen.

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.

AWV speelt een cruciale rol binnen dit programma. Het programma realiseerde een platform dat intelligente 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.

Om deze nieuwe of verbeterde diensten aan de weggebruikers te kunnen verlenen, rekent [AWV] 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.

[Service Provider] 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 [AWV] en [Service Provider] uitwisselen als verwerkingsverantwoordelijken.

De gegevensstromen vallen uiteen in volgende grote stromen:

1. Prioriteitsaanvragen-stroom (SREM-berichten en CAM-berichten) van [Service Provider] naar Mobilidata Interchange en TLEX van [AWV] en omgekeerd (SSEM-berichten)
 2. Weggebruikerposities-stroom voor waarschuwingen (DENM-berichten) van [Service Provider] naar Mobilidata Interchange van [AWV]
- 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 [AWV] 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 [Service Provider] heeft in de periode september 2024 t.e.m. augustus 2025 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 [AWV] en [Service Provider] uiteengezet.

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

Artikel 2.1: Beoogde verwerking door [AWV]

Artikel 2.1.1: Beoogde verwerking door [AWV] van Prioriteitsaanvragen

De beoogde gegevensverwerking door [AWV] gebeurt op grond van

- Artikel 6.1.e, in het kader van een taak van algemeen belang om het verkeer veiliger te maken door prioritaire voertuigen groen licht te geven en het doorgeven van gegevens naar betrokken wegbeheerders.

[Service Provider] 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.

[AWV] zal de opgevraagde gegevens verwerken voor volgende doeleinden:

- Het verlenen van prioriteit aan specifieke weggebruikers op geconnecteerde kruispunten.
- Het doorgeven van verkeersinformatie aan aangesloten wegbeheerders
- 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 [AWV] is verenigbaar met de doeleinden waarvoor [Service Provider] de gegevens oorspronkelijk heeft verzameld, gezien prioriteitsverlening het doel van de oorspronkelijke verwerking is.

Artikel 2.1.2: Beoogde verwerking door [AWV] van Verkeersinformatie-berichtenstroom met weggebruikerposities voor waarschuwingen

De beoogde gegevensverwerking door [AWV] gebeurt op grond van

- Artikel 6 1 e, taak van algemeen belang, om het verkeer veiliger te maken door het uitsturen van waarschuwingen naar weggebruikers en het doorgeven van gegevens naar betrokken wegbeheerders

[Service Provider] heeft de opgevraagde gegevens oorspronkelijk verzameld voor volgende doeleinden

- het leveren en verbeteren van verkeersinformatiediensten aan bij haar aangesloten weggebruikers, en bijvoorbeeld voor het waarschuwen van weggebruikers voor
 - o stilstaande of aankomende hulpdiensten

[AWV] zal de opgevraagde gegevens verwerken voor volgende doeleinden:

- het leveren en verbeteren van verkeersinformatiediensten aan weggebruikers, en bijvoorbeeld voor het waarschuwen van weggebruikers voor
 - o stilstaande of aankomende hulpdiensten
- Het doorgeven van verkeersinformatie aan aangesloten wegbeheerders
- Verdere verwerking, het aggregeren en daarna archiveren voor verder onderzoek en beleidsevaluatie

Het doeleinde van de verdere verwerking van deze persoonsgegevens door [AWV] is verenigbaar met de doeleinden waarvoor [Service Provider] de gegevens oorspronkelijk heeft verzameld, gezien de doelen overeenkomen

Artikel 2.2: Beoogde verwerking door [Service Provider]

Artikel 2.2.1: Beoogde verwerking door [Service Provider] van Prioriteitsaanvragen

[Service Provider] ontvangt enkel berichten van type SSEM, welke betrekking hebben op de status van afhandeling van een geconnecteerd verkeerslicht die hoort bij een specifieke verstuurde Prioriteitsaanvraag, en die de originele aanvraag-gegevens bevat, afkomstig van [Service Provider]

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:	Persoonsgegevens in de Verkeersinformatie-berichtenstroom zijn:
-------------------	---

Verkeersinformatie-berichtenstroom, met weggebruikerposities voor waarschuwingen [DENMs]	- Pseudoniem ID - Real-time verplaatsingsgegevens van prioritaire voertuigen en (indien gekend) type van prioritair voertuig - Real-time verplaatsingsgegevens van traag rijdende of stilstaande prioritaire voertuigen
Verantwoording proportionaliteit	De gegevens uit de verkeersinformatiestroom met weggebruikerposities (real-time verplaatsingsgegevens) voor waarschuwingen [DENMs] zijn noodzakelijk om - Weggebruikers aangesloten bij andere aangesloten instanties te kunnen waarschuwen voor de aanwezigheid en mogelijk gevaar; - en hierdoor ook het risico op ongeval voor de betrokkene zelf te verkleinen
Gegeven 2 Prioriteitsaanvragen-stroom [SREMs, SSEM's en CAMs]	Prioriteitsaanvragen-stroom [SRMs, SRMs en CAMs] bevat volgende persoonsgegevens: - Pseudoniem ID - 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 konvooien.

--	--

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

Gegeven	Maximale bewaartermijn	Verantwoording
Gegeven 1 Verkeersinformatieberichten, met weggebruikerposities voor waarschuwingen [DENMs]	6 maanden	6 maanden worden ingeschat als nodig voor het analyseren verbeteren en verzekeren van het goed uitsturen van waarschuwingen
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.

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

Artikel 4.1: Door [AWV]

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

- Volgende diensten van [AWV] zullen toegang hebben tot de gevraagde persoonsgegevens.
 - o Alle afdeling van [AWV]

Enkel personen die omwille van hun functieprofiel 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 [AWV] – leveranciers van verkeersregelingen en verkeersinformatiediensten
 - o Lokale wegbeheerders (voor de gegevens op de door hen beheerde wegen)

Elke eventuele mededeling van de gevraagde persoonsgegevens door [AWV] moet voorafgaandelijk aan [Service Provider] 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 [AWV] waar vereist een protocol sluit voor de mededeling van de gevraagde gegevens

Artikel 4.2: Door [Service Provider]

[Service Provider] ontvangt enkel SSEM berichten, en dus geen nieuwe persoonsgegevens van [AWV].

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 voor onbepaalde duur.

Artikel 6: Beveiligingsmaatregelen

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

Artikel 6.1: Beveiligingsmaatregelen door [AWV]

- 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

[AWV] 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.

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

In het geval [AWV] voor de verwerking van persoonsgegevens die het voorwerp zijn van voorliggend protocol, beroep doet op een verwerker (of meerdere verwerkers), doet de [AWV] 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. [AWV] 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 Service Provider

De [Service Provider] treft ten minste volgende organisatorische en technische beveiligingsmaatregelen ter beveiliging van de ontvangen persoonsgegevens bij verdere verwerking:

Organisatorische	beveiligingsmaatregelen:
"Awareness" - medewerkers van JdSoft zijn zich bewust van de manier waarop er omgegaan dient te worden met de persoonsgegevens. JdSoft heeft ook de nodige maatregelen getroffen wat betreft de toegang en restricties betreffende persoonlijke gegevensverwerking. Er is een duidelijke communicatie naar werknemers & partners met een "non-disclosure agreement". Afspraken en een bedrijfspolicy zijn beschreven voor developers en werknemers betreffende persoonlijke gegevensverwerking. Er is een GDPR overeenkomst afgesloten met haar "hosting-partner" Google cloud. JdSoft zal onder geen beding persoonsgegevens verstrekken aan een derde partij zonder de specifieke aanvraag van de Verantwoordelijke voor de verwerking.	

Technische	beveiligingsmaatregelen:
Alle gegevens worden geencrypteerd opgeslagen in de database. Alle data wordt over een beveiligde SSL verbinding verstuurd met een end-to-end certificaat. De software gebruikt "rollen" met bevoegdheden om de restricties te bepalen in de applicatie. Gevoelige persoonlijke data wordt geencrypteerd in de historie van de applicatie en heeft een admin paswoord nodig om getoond te worden. Alle acties in de applicatie worden gelogd en bijgehouden op gebruikers niveau. De database zelf is ook geencrypteerd en dus niet leesbaar als tekst zonder gebruik van de applicatie.	

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

In het geval [Service Provider] voor de verwerking van persoonsgegevens die het voorwerp zijn van voorliggend protocol, beroep doet op een verwerker (of meerdere verwerkers), doet de [Service Provider] 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. [Service Provider] 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 persoonsgegevens

Zodra [AWV] of [Service Provider] één of meerdere foutieve, onnauwkeurige, onvolledige, ontbrekende, verouderde of overtollige 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 [Service Provider] of [AWV] 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 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 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: Transparantie

Partijen informeren de betrokkenen, in het licht van het transparantiebeginsel van de algemene verordening, via publicatie op hun website.

Dit protocol zal door AWW worden gepubliceerd via <https://www.wegenenverkeer.be/privacy>.

Dit protocol zal door [Service Provider] worden gepubliceerd via <https://jdsoft.be> en <https://fireplug.be>.

Daarnaast worden de betrokkenen bijkomend geïnformeerd over het programma Mobilidata via de website www.mobilidata.be.

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 vanaf ondertekening door beide partijen van zowel dit protocol als de Mobilidata Interchange aansluitovereenkomst voor [Service Provider].

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 14: 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.

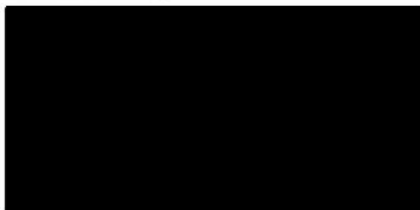
Aangezien deze overeenkomst digitaal wordt ondertekend, wordt in overeenstemming met artikel 8.20 NBW slechts één (digitaal) exemplaar van deze overeenkomst opgemaakt.

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.

administrateur-generaal

Kathy Vandenmeersschaut

[namens AWV]



Bestuurder / CEO

Jan Van Hooydonck



MOBILIDATA INTERCHANGE AANSLUIT OVEREENKOMST

Tussen

Het VLAAMSE GEWEST,

in deze vertegenwoordigd door de Vlaamse regering, bij delegatie in hoofde van mevr. Annick De Ridder, Vlaams minister voor Mobiliteit, Openbare Werken, Havens en Sport,

in deze bij delegatie vertegenwoordigd door mevr. ir. Kathy Vandenmeersschaut, in haar hoedanigheid van administrateur-generaal van het intern verzelfstandigd zonder rechtspersoonlijkheid

Agentschap Wegen en Verkeer,

entiteit ingeschreven in de Kruispuntbank Ondernemingen onder het ondernemingsnummer 0316.380.841 met vestigingseenheid te 1000 BRUSSEL, Simon Bolivarlaan 17 bus 420

Hierna: 'AWV'

en

C-ITS DIENSTVERLENER

JdSoft bv, vertegenwoordigd door Jan Van Hooydonck, ingeschreven in het KBO met nummer BE0460.831.756, waarvan de administratieve zetel zich bevindt te Vaartstraat 17, 2960 Brecht

Hierna de "C-ITS Service Provider",

Bovenstaande partijen worden hieronder ook wel afzonderlijk aangeduid als een "Partij" of gezamenlijk als de "Partijen";

Preambule

De Partijen gaan een overeenkomst aan inzake:

Mobilidata Interchange Aansluiting.

Deze overeenkomst is opgesteld in het Nederlands. In geval van discrepanties of onduidelijkheden tussen de Nederlandse tekst en een vertaling, is de Nederlandse tekst leidend en bepalend voor de interpretatie van deze overeenkomst.

Overwegende dat Mobilidata een programma is van de Vlaamse Regio in een partnerschap tussen meerdere Vlaamse Overheden en imec., waarin AWV de uitvoering verzorgt, wordt de Mobilidata Interchange door AWV beheerd, en aansluitingsovereenkomsten met AWV afgesloten;

Overwegende dat Mobilidata innovatieve verkeersoplossingen realiseert in samenwerking met private partners; dat deze verkeersoplossingen worden gerealiseerd op basis van een digitale infrastructuur, intelligente verkeerslichten en hoogwaardige, duurzame databronnen;

Overwegende dat de C-ITS Service Provider een software ontwikkeld heeft voor de alarmering en dispatching van medische dringende hulpdiensten via de verwittiging van de Noodcentrales 112, en oplossingen aanbiedt om snel, efficiënt maar vooral veilig de first responders en hulpverleners ter plaatse te brengen;

Overwegende dat de Partijen elkaar willen aanspreken met betrekking tot een verbinding met het Mobilidata Ecosysteem en overeenkomen dat deze verbinding zal plaatsvinden zoals beschreven in de rest van deze aansluitingsovereenkomst (hierna de "Overeenkomst"), die de modaliteiten en voorwaarden bepaalt waaronder zij de aansluiting vorm willen geven, inclusief de rechten, rollen en plichten van beide Partijen.

Komen het volgende overeen:

Artikel 1. Definities

In het kader van deze overeenkomst hebben de volgende begrippen onderstaande betekenis:

1.1. **Betrokkene:** zie AVG

1.2. **C-ITS Information Provider:** Een Partij die informatie verstrekt aan weggebruikers via diensten of toepassingen.

1.3. C-ITS Service Provider: Een Partij die verbinding maakt met de Mobilidata informatiestroom en deze informatie verwerkt of voorbereid voor verdere toepassingen voor weggebruikers. Deze rol kan gecombineerd worden met die van C-ITS Information Provider.

1.4. C-Roads Standaarden: Europese standaarden voor coöperatieve, verbonden en geautomatiseerde mobiliteitsdiensten, gehanteerd binnen het Mobilidata-programma.

1.5. Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt of kan leiden tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.6. Gebruiker: eindgebruiker van een toepassing van een C-ITS Informatieprovider.

1.7. Gegevens: Alle informatie, data of datasets, inclusief maar niet beperkt tot verkeersgerelateerde data, real-time en/of near-time informatie, statistieken, en andere relevante informatie die door een Partij of diens Gelieerde Onderneming wordt verstrekt, gedeeld of beschikbaar gesteld via de Mobilidata Interchange, voor zover deze betrekking hebben op de uitvoering van de use cases binnen het kader van deze Overeenkomst.

1.8. Gegevensuitwisseling: De overdracht van real-time en/of near-time verkeersdata tussen de Partijen voor de overeengekomen doeleinden.

1.9. Mobilidata: Het data-uitwisselingsprogramma van AWW dat gericht is op de verbetering van de verkeersveiligheid, doorstroming en milieu-impact in het Vlaamse mobiliteitslandschap.

1.10. Mobilidata Ecosysteem: Het netwerk van verkeers- en gegevensdiensten in Vlaanderen, dat alle wegen omvat (snelwegen, regionale en lokale wegen). Het ecosysteem ondersteunt verschillende weggebruikers (fietzers, automobilisten, openbaar vervoer, hulpdiensten, enz.) en biedt dataservices voor 29 C-ITS-gebruikscasussen. AWW is de belangrijkste overheidsdeelnemer, met private dienstverleners die zijn verbonden aan de Mobilidata Interchange.

1.11. Mobilidata Interchange: De centrale informatiehub die Mobilidata verbindt met C-ITS Service Providers.

1.12. Use Cases: Specifieke toepassingen waarvoor de gegevensuitwisseling plaatsvindt, zoals omschreven in de Bijlage 1 bij deze Overeenkomst.

1.13. Vermoed datalek: een vermoeden van een mogelijke inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze kan leiden tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, waarvan in het kader van het onderzoek van de Verwerker naar het Vermoed datalek nog niet redelijkerwijze vastgesteld kon worden dat er daadwerkelijk een Datalek heeft plaatsgevonden. Een Vermoed datalek kwalificeert dus (nog) niet als een Datalek. De verplichtingen met betrekking tot de behandeling en melding van een Datalek opgenomen in de verwerkersovereenkomst en de wetgeving gegevensbescherming eindigen pas na redelijkerwijze kan aangetoond worden dat er geen sprake is van een Datalek.

1.14. Verwerkingverantwoordelijke: Zie AVG

1.15. Vertrouwelijke Informatie: Alle informatie die door een Partij aan de andere wordt verstrekt, ongeacht de vorm, die als vertrouwelijk wordt aangeduid. Indien schriftelijk of elektronisch, moet de informatie als "vertrouwelijk" worden gemarkeerd. Mondelinge vertrouwelijke informatie moet schriftelijk als vertrouwelijk worden bevestigd door de verstrekende Partij.

Artikel 2: Doel

2.1. Verkeersgerelateerde Use Cases:

De Partijen komen overeen om samen te werken met als doel innovatieve technologische verkeersoplossingen aan weggebruikers te bieden door het delen van real-time en/of near-time relevante gegevens via de Mobilidata Interchange. Deze gegevensuitwisseling vindt plaats binnen het kader van de overeengekomen use cases, die expliciet zijn beschreven en geformuleerd door AWW in bijlage 1.

2.2. Gegevensuitwisseling:

a) AWW stelt de Mobilidata Interchange beschikbaar voor de C-ITS Service Provider en

b) AWW stelt verkeersgerelateerde gegevens beschikbaar via de Mobilidata Interchange aan aangesloten partijen, met inachtneming van de beperkingen en verplichtingen van deze overeenkomst en met volledige naleving van de toepasselijke wet- en regelgeving, met inbegrip van, maar niet beperkt tot, de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679). Deze gegevens mogen uitsluitend worden gebruikt binnen het kader van de overeengekomen Use Cases en doelstellingen, gericht op de verbetering van verkeersveiligheid, doorstroming en het verhogen van de duurzaamheid. Het gebruik van de gegevens voor andere doeleinden dan in deze overeenkomst is uitsluitend toegestaan met de voorafgaande schriftelijke toestemming van AWW.

c) De C-ITS Service Provider kan op zijn beurt eigen gegevens verzamelen via zijn gebruikers en systemen, en kan deze gegevens delen met AWW door ze beschikbaar te stellen via de Mobilidata Interchange. Deze bijdrage zal het beschikbare gegevensaanbod binnen de Mobilidata Interchange vergroten en de mogelijkheden voor verdere innovaties verbeteren.

2.3 Inspanningsverbintenis:

De Partijen delen verkeersgerelateerde gegevens met elkaar volgens een inspanningsverbintenis, zowel voor het delen van de gegevens als voor de correctheid van deze gegevens.

2.4. Kosten en vergoedingen

De samenwerking is kosteloos. Elke Partij draagt zijn eigen kosten voor de uitvoering van deze overeenkomst. Geen van de Partijen ontvangt van de andere Partij(en) financiële compensatie voor de gegevens die via de Mobilidata Interchange worden ter beschikking gesteld. Dit sluit evenwel niet uit dat een Partij aansprakelijk kan worden gesteld voor schade die de andere Partij lijdt, indien en voor zover deze schade het gevolg is van een schending van deze overeenkomst of van toepasselijke wet- en regelgeving.

Artikel 3: Ingangsdatum en duur

3.1. Deze Overeenkomst treedt in werking op de datum van ondertekening en wordt aangegaan voor onbepaalde duur.

3.2. Beëindiging

Elke Partij kan de overeenkomst te allen tijde beëindigen, onder de volgende voorwaarden:

Zonder opgave van reden, met een opzegtermijn van drie (3) maanden, per aangetekende brief;

Bij dringende redenen kan elke Partij de overeenkomst zonder opzegtermijn en zonder gerechtelijke tussenkomst beëindigen in geval van ernstige tekortkomingen van de andere Partij. Dringende redenen omvatten, maar zijn niet beperkt tot:

a) Onvoldoende datakwaliteit geleverd door de C-ITS Service Provider. In dit geval kan de Mobilidata Interchange-verbinding tijdelijk worden afgekoppeld, en bij aanhoudende tekortkomingen definitief worden beëindigd;

Er is sprake van onvoldoende datakwaliteit in onder meer de volgende gevallen:

- het frequent genereren van foutieve meldingen, waaronder vals-positieve of vals-negatieve waarschuwingen;
- het niet tijdig afmelden van prioriteitsverzoeken;
- onnauwkeurige, onvolledige of verouderde gegevens die de betrouwbaarheid van de C-ITS-diensten in het gedrang brengen.

b) Niet-naleving van de vigerende wet- en regelgeving;

c) Gebruik van de gegevens voor niet-goedgekeurde doeleinden. De C-ITS Service Provider mag de gegevens alleen gebruiken binnen het kader van de overeengekomen use cases. Voor ander gebruik is voorafgaande schriftelijke toestemming van AWW vereist

In geval van ernstige tekortkomingen die niet onder de dringende redenen vallen, dient een ingebrekestelling per aangetekende brief te worden gestuurd, met een herstelperiode van dertig (30) kalenderdagen. Indien er binnen deze periode geen adequate correctie plaatsvindt, kan de overeenkomst worden beëindigd. De herstelperiode kan worden verlengd indien de andere Partij aantoonbaar en op redelijke wijze werkt aan het herstel.

Elke Partij heeft het recht om de overeenkomst onmiddellijk en zonder opzegtermijn te beëindigen in geval van faillissement, ontbinding, liquidatie, staking van betalingen, of fraude van de andere Partij.

3.3. Procedure van Beëindiging

Beëindiging op grond van de bovenstaande redenen moet schriftelijk worden gemotiveerd. De beëindiging van de overeenkomst heeft geen invloed op reeds lopende verplichtingen tussen partijen met betrekking tot de reeds uitgewisselde gegevens.

Artikel 4: Use cases

4.1. Verkeersgerelateerde Use Cases

De uitwisseling van gegevens in het kader van deze overeenkomst is beperkt tot real-time en/of near-time verkeersinformatie die specifiek betrekking heeft op de overeengekomen use cases. Deze use cases worden in detail beschreven in de Bijlage 1 bij deze overeenkomst.

4.2. Use Cases met persoonsgegevens:

Verschillende verkeersgerelateerde use cases bevatten gegevens die rechtstreeks of onrechtstreeks herleidbaar zijn tot individuele verkeersdeelnemers. Voor het verwerken van deze gegevens is een hoge mate van zorgvuldigheid vereist.

De Partijen hebben in deze uitwisseling elk de hoedanigheid van Verwerkingverantwoordelijke voor de eigen verwerkingen. Partijen dienen voorafgaand aan de uitwisseling van deze gegevens een protocol af te sluiten. Er worden geen gezamenlijke verwerkingen voorzien.

Artikel 5: Specificaties

AWV hanteert zo veel mogelijk de C-Roads specificaties voor de uitwisseling van verkeersdata in het kader van Mobilidata. Deze specificaties zijn ontwikkeld binnen een Europees samenwerkingsproject en bevorderen de interoperabiliteit en veiligheid van Coöperatieve Intelligente Transport Systemen (C-ITS). Het doel is om interoperabele grensoverschrijdende C-ITS diensten voor weggebruikers te realiseren. C-ITS stelt voertuigen in staat om direct met elkaar en de omliggende weginfrastructuur te communiceren.

Voorlopige lokale afwijkingen van de C-Roads specificaties, met betrekking tot de verkeerslichten use cases en de ondertekening van berichten, worden verduidelijkt in de beschikbare technische documentatie.

Van de C-ITS Service Provider wordt verwacht dat zij de C-Roads specificaties volgt bij de implementatie en uitvoering van de overeengekomen use cases. AWV behoudt zich echter het recht voor om niet automatisch elke nieuwe versie van de C-Roads specificaties te implementeren. Indien AWV ervoor kiest om een nieuwe versie van de C-Roads specificaties te volgen, zal de C-ITS Service Provider op basis van overleg de nodige acties ondernemen om tijdig aan deze nieuwe versie te voldoen. Hierbij zal in onderling overleg een planning worden vastgesteld om de implementatie te realiseren.

Artikel 6: Modaliteiten van Toestemming en Gegevensverzameling

6.1. Toestemming voor Gegevensverwerking

De C-ITS Service Provider is verplicht om, waar van toepassing, de vereiste toestemming van de Betrokkene te verkrijgen voor het verzamelen en verwerken van gegevens in het kader van de overeengekomen use cases. Dit betreft met name de verwerking van persoonsgegevens en andere privacygevoelige gegevens. De C-ITS Service Provider dient ervoor te zorgen dat deze toestemmingsprocedures volledig voldoen aan de geldende privacywetgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), bij gebreke waaraan de C-ITS Service Provider AWV zal vrijwaren voor enige schade inclusief schadevorderingen van een gebruiker als gevolg van het niet respecteren van de bepalingen inzake toestemming voor gegevensverwerking.

De Betrokkene wordt voorafgaand het verkrijgen van de toestemming duidelijk geïnformeerd over de doorgifte van gegevens aan wegbeheerders en over de doeleinden van de verwerking door deze wegbeheerders, zoals beschreven in artikel 2. Zowel de verstrekking als de intrekking van de toestemming wordt nauwkeurig geregistreerd, zodat deze ten alle tijde kan worden getraceerd. De informatie over de doorgifte en de doeleinden van verwerking blijven voor de Betrokkene raadpleegbaar, ook na het geven van de toestemming.

De C-ITS Service Provider is verplicht om alle verplichtingen uit de AVG inzake toestemming na te leven (onder meer maar niet beperkt tot art. 7, 8, 9 lid 2, a), 13 lid 2, c), 17 lid 1, b), 18 lid 2).

De toestemming dient actief door de Betrokkene te worden verleend door middel van een opt-in systeem, waarbij de standaardinstelling is dat toestemming niet is gegeven.

Indien de gegevens van de Betrokkene worden verkregen via een derde partij, is de C-ITS Service Provider verplicht contractuele afspraken te maken met deze derde partij om ervoor te zorgen dat deze partij zich houdt aan dezelfde voorwaarden ten aanzien van toestemming en gegevensverwerking als de C-ITS Service Provider zelf bij gebreke waaraan de C-ITS Service Provider AWV zal vrijwaren voor enige schade inclusief schadevorderingen van een gebruiker als gevolg het ontbreken of niet respecteren van deze contractuele afspraken op vlak van toestemming en gegevensverwerking.

6.2. Voorwaarden voor Gegevensverzameling en Gebruik

De C-ITS Service Provider moet aan de volgende voorwaarden voldoen bij het verzamelen en gebruiken van gegevens in het kader van de overeengekomen use cases:

- a) De C-ITS Service Provider is verantwoordelijk voor het duidelijk informeren van de Betrokkenen over de aard van de verzamelde gegevens, het doel van de verzameling, en de wijze waarop de gegevens worden gedeeld met wegbeheerders, in overeenstemming met het transparantiebeginsel. De informatie moet begrijpelijk en gemakkelijk toegankelijk zijn voor de Betrokkenen;
- b) Beperking tot overeengekomen use cases. Indien de C-ITS Service Provider de Use Cases wenst uit te breiden, dienen hierover nieuwe onderhandelingen plaats te vinden;
- c) De C-ITS Service Provider mag alleen de minimale hoeveelheid gegevens verzamelen die noodzakelijk is voor de uitvoering van de overeengekomen use cases, in overeenstemming met het principe van data minimalisatie en doelbinding.

6.3. Documentatie en verantwoording

De C-ITS Service Provider is verplicht om stavende documentatie bij te houden van de toestemmingen die zijn verkregen van Betrokkenen, evenals van de data die verzameld en gedeeld wordt in het kader van de use cases. Deze documentatie moet op verzoek beschikbaar worden gesteld aan AWV voor audit- en nalevingsdoeleinden.

6.4. Naleving en Verantwoordelijkheid

De C-ITS Service Provider is verantwoordelijk voor het naleven van alle wettelijke en contractuele verplichtingen met betrekking tot de toestemming van Betrokkenen en de verwerking van gegevens. Indien blijkt dat de C-ITS Service Provider deze verplichtingen niet naleeft, behoudt AWV zich het recht

voor om de toegang tot de Mobilidata Interchange tijdelijk te schorsen of de overeenkomst te ontbinden, zoals beschreven in Artikel 3 van deze Overeenkomst.

Artikel 7: Bewaartermijnen en vernietiging van Persoonsgegevens

7.1. Bewaartermijnen van Persoonsgegevens

De bewaartermijnen voor de door elke Partij aangeleverde persoonsgegevens zullen worden vastgelegd in een gezamenlijk protocol. Iedere Partij blijft verantwoordelijk voor de rechtvaardiging van zijn eigen bewaartermijnen. Elke Partij zal persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt, niet langer bewaren dan noodzakelijk is voor het vervullen van de overeengekomen Use Cases en de doelen van deze Overeenkomst, tenzij een langere bewaartermijn wettelijk verplicht is.

7.2. Vernietiging van Persoonsgegevens

Na afloop van de toepasselijke bewaartermijn of wanneer de gegevens niet langer nodig zijn voor de overeengekomen doeleinden, zullen de Partijen alle persoonsgegevens op veilige wijze vernietigen.

7.3. Documentatie van Vernietiging

Elke Partij dient op verzoek van de andere Partij schriftelijk bewijs te leveren van de vernietiging van de persoonsgegevens. Dit bewijs moet in detail de aard van de vernietigde gegevens, de datum van vernietiging en de methode van vernietiging vermelden.

7.4. Uitzonderingen

Indien een Partij wettelijk verplicht is om persoonsgegevens langer te bewaren dan de overeengekomen bewaartermijn, zal die Partij de andere Partij daarvan schriftelijk op de hoogte stellen, inclusief de reden en de duur van de verlengde bewaartermijn. De verwerking van deze gegevens blijft onderworpen aan de bepalingen van deze Overeenkomst en de toepasselijke wetgeving.

7.5. Beveiliging van Gegevens tijdens de Bewaartermijnen

Tijdens de bewaartermijn zullen de Partijen passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking, verlies, vernietiging of schade, in overeenstemming met de geldende privacywetgeving en de beste beveiligingsstandaarden.

Artikel 8: Rechten en Rollen voor Specifieke Organisaties

Specifieke Organisaties kunnen recht hebben op toegang tot specifieke use cases voor het vervullen van hun operationele taken. De aard en mate van toegang kunnen variëren naargelang de use case.

8.1 Types Specifieke Organisaties

- Organisaties met en eigenaars van prioritaire voertuigen
- Organisaties, bedrijven en eigenaars van
 - Bussen voor openbaar vervoer
 - Tram/metrostellen
 - Dienstvoertuigen (voertuigen met oranje-gele knipperlichten), o.a. maar niet beperkt tot
 - Afschermende voertuigen met botsabsorbers
 - Werfvoertuigen
 - Winterdienstvoertuigen
 - Takeldiensten
 - Dienstwagens wegbeheerder

8.2. Minimale Voorwaarden en Verantwoordelijkheden

De minimale voorwaarden voor aansluiting van Specifieke Organisaties, met specifieke eisen voor rechtenbeheer, voertuigen en devices, zijn opgenomen onder bijlage 5. Onder deze voorwaarden staat AWW toe dat de C-ITS Service Provider de diensten uit 8.3.d aanbiedt aan Specifieke Organisaties en hun devices/voertuigen.

8.3. Validatie en Authenticatie van Voertuigen

De Partijen verbinden zich ertoe om de nodige stappen te ondernemen die de validiteit en authenticiteit van specifieke voertuigen te waarborgen.

a) Documentatie en Verificatie:

De C-ITS Service Provider is verantwoordelijk voor het beheer van de voertuigregistratie en voor de juistheid van de voertuigtypes, waarbij hij gebruikmaakt van een of meer methodes uit bijlage 2.

b) Toekennen en Beheren van Rechten

Rechten en toezicht voor aanvragers worden beheerd door de C-ITS Service Provider, die tevens zorgt voor een correcte registratie van de organisatie- en contactinformatie van de aanvrager, inclusief het aantal en type voertuigen en de gewenste ingangsdatum.

De C-ITS Service Provider dient het proces en beleid m.b.t. toekenning van rechten en autorisatie voor voertuigen/devices te beschrijven en ter goedkeuring voor te leggen aan AWW. De C-ITS Service Provider neemt in haar overeenkomsten met Specifieke Organisaties de nodige voorwaarden op zodat de minimale voorwaarden van AWW voor het toekennen en beheren van voertuigrechten worden nageleefd.

Er vindt een kwartaalrapportage plaats naar AWW waarin de aangesloten partijen, voertuigen, voertuigtypes en eventuele incidenten ten aanzien van beleid worden gerapporteerd.

c) Periodieke Audit en Jaarlijkse Review

C-ITS Service Provider laat het proces voor toekenning van de rechten auditen door een onafhankelijke auditor binnen 6 maanden na de eerste toekenning, en daarna elke 2 jaar. Kosten voor deze audit vallen ten laste van de C-ITS Service Provider. Het audit rapport wordt aan AWW bezorgd.

AWV of een onafhankelijke auditor kan ad hoc controles uitvoeren indien afwijkend gedrag zich stelt of naar aanleiding van eventuele meldingen of klachten. Bij constatering van afwijkend gedrag zal het desbetreffende voertuig(en) afgekoppeld worden van het systeem.

Jaarlijks beoordeelt de C-ITS Service Provider de accuraatheid van de gegevens en verlengt de rechten van de vloot indien nodig. De C-ITS Service Provider verifieert hiervoor de gegevens bij de Specifieke Organisaties.

d) Prioriteit- en Toegangsrechten

Prioritaire voertuigen kunnen absolute prioriteit aanvragen bij geconnecteerde verkeerslichten van AWW en aangesloten wegbeheerders, en kunnen waarschuwingen versturen.

Dienstvoertuigen kunnen waarschuwingen versturen, naargelang het type dienstvoertuig.

Voertuigen voor openbaar vervoer kunnen conditionele prioriteit aanvragen op geconnecteerde verkeerslichten van AWW en aangesloten wegbeheerders (conditioneel: met een weging naargelang beleid bij optimalisatie van de verkeersregeling)

Artikel 9: Licentie voor gegevensgebruik

9.1. Gegevenslicentie aan AWW

De C-ITS Service Provider verleent aan AWW een niet-exclusief, kosteloosrecht om de gegevens die hij op de Mobilidata Interchange ter beschikking stelt te gebruiken in verband met de AWW-gebruikssituaties. Deze licentie omvat tevens het recht voor AWW om de verzamelde gegevens te archiveren voor het doel, voor wetenschappelijk onderzoek en voor beleidsvoorbereiding. AWW kan de gearchiveerde gegevens voor deze doeleinden delen met partners. AWW heeft bovendien het recht om de gearchiveerde gegevens na afloop van de overeenkomst te behouden en te blijven gebruiken, voor zover de intellectuele eigendomsrechten op de betreffende gegevens van toepassing blijven. Deze licentie wordt verleend voor een onbepaalde duur, waarbij de licentie blijft gelden zolang de intellectuele eigendomsrechten op de betreffende gegevens van toepassing zijn.

9.2. Datalicentie aan de C-ITS Service Provider

Aan de C-ITS-Provider wordt een niet-exclusief recht verleend om de niet-persoonsgebonden gegevens te gebruiken voor de overeengekomen Use Cases, met inbegrip van de overdracht, publicatie en commerciële exploitatie van het product. Dit gebruiksrecht is uitsluitend van toepassing op gegevens die geen persoonsgegevens zijn in de zin van de Algemene Verordening Gegevensbescherming (AVG).

In het bijzonder, en gelet op de verplichtingen die de C-ITS Service Provider krachtens deze Overeenkomst op zich neemt, verleent AWW de C-ITS Service Provider de volgende rechten:

i. Het recht op toegang tot de niet-persoonsgebonden gegevens en andere door AWW geleverde diensten, strikt beperkt tot de verwezenlijking van het Doel en de overeengekomen Use Cases, gedurende de looptijd van deze Overeenkomst;

ii. Het recht om de niet-persoonsgebonden gegevens door te geven aan derden, in overeenstemming met de toepasselijke wet- en regelgeving.

9.2.1. Onrechtmatig hergebruik van gegevens

Onrechtmatig hergebruik van de gegevens (ongeacht of het persoonsgegevens of niet-persoonsgegevens betreft) is verboden. De C-ITS Service Provider verbindt zich ertoe de toepasselijke regelgeving inzake gegevensbescherming, waaronder de AVG, volledig na te leven bij het hergebruik van gegevens.

9.2.2. Met betrekking tot persoonsgegevens

Voor zover de gedeelde gegevens persoonsgegevens bevatten, mogen deze uitsluitend worden verwerkt voor de overeengekomen Use Cases en enkel in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming. Ter verduidelijking: de aan de C-ITS Service Provider verleende

rechten krachtens deze Overeenkomst hebben uitsluitend betrekking op niet-persoonsgebonden gegevens. De C-ITS Service Provider is als enige verantwoordelijk voor de verwerking van persoonsgegevens.

Commercieel hergebruik, verdere publicatie of doorgifte van persoonsgegevens aan derden is enkel toegestaan voor zover dit in overeenstemming is met de toepasselijke regelgeving inzake gegevensbescherming, waaronder doch niet beperkt tot de AVG. De ontvanger is als enige verantwoordelijk voor het waarborgen dat elke verwerking of verdere doorgifte rechtmatig is en in overeenstemming met de toepasselijke bepalingen van de Standaardcontractbepalingen.

9.2.3. Toepasselijke voorwaarden bij doorgifte aan derden

Voor zowel persoonsgegevens als niet-persoonsgebonden gegevens geldt dat, wanneer de C-ITS Service Provider gegevens doorgeeft aan een derde partij, deze derde partij, via een overeenkomst of een andere juridische handeling onder het Unierecht of het nationale recht, aan dezelfde verplichtingen en voorwaarden moet worden onderworpen als die welke op de C-ITS Service Provider rusten krachtens deze Overeenkomst.

In het bijzonder moet de C-ITS Service Provider ervoor zorgen dat elke dergelijke doorgifte voldoet aan Hoofdstuk V van de AVG en onderworpen is aan passende waarborgen, en moet hij AWW vooraf informeren over de identiteit van de derde partij en het doel van de verdere doorgifte.

9.2.4. Beperking van de licentie

Deze licentie is bovendien alleen geldig voor de duur van de huidige Overeenkomst. De C-ITS Service Provider erkent en stemt ermee in dat de gegevenslicentie onderhevig is aan de beperkingen zoals gedefinieerd in de huidige Overeenkomst en stemt ermee in dat hij en derden te allen tijde zullen voldoen aan deze licentie.

De C-ITS Service Provider zal de gegevens alleen voor het toegestane gebruik gebruiken en zal niet, zonder voorafgaande schriftelijke toestemming van AWW, onder geen enkele omstandigheid het gebruik of de toestemming voor het gebruik aan Derden voor enig ander doel dan het Doel zoals gedefinieerd in de huidige Overeenkomst toestaan.

9.2.5. Bewaring en verwijdering van gegevens

De bewaartermijnen worden strikt gerespecteerd en na het verstrijken ervan worden de gegevens verwijderd of geanonimiseerd, in overeenstemming met de wettelijke verplichtingen en de bepalingen van deze Overeenkomst. Elke schending hiervan zal resulteren in de beëindiging van de Overeenkomst volgens artikel 3.2.

9.2.6. Naleving van voorwaarden

De C-ITS Service Provider zorgt voor de naleving van de voorwaarden en bepalingen zoals uiteengezet in deze Overeenkomst, inclusief de verplichting tot back-to-back contracteren van alle relevante bepalingen over gegevensgebruik en gegevensdeling in contracten met derden.

Artikel 10: Incidenten en datalekken

10.1. Melding van een vermoed datalek

De partijen informeren elkaar zo snel mogelijk en uiterlijk binnen 24 uur nadat zij kennis hebben genomen van een vermoed datalek of een effectief datalek. De melding gebeurt op een manier die de desbetreffende partij in staat stelt tijdig te voldoen aan de wettelijke verplichtingen onder de wetgeving gegevensbescherming.

De partijen verstrekken in geval van een datalek in verband met persoonsgegevens alle relevante informatie aan elkaar met betrekking tot dit datalek, waaronder de aard van het datalek in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevens in kwestie en, bij benadering, het aantal betrokkenen en het aantal persoonsgegevens in kwestie; de waarschijnlijke gevolgen van het datalek in verband met persoonsgegevens; en de maatregelen die zij hebben voorgesteld of genomen hebben om het datalek in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

10.2. Maatregelen ter beperking van de schade

De partijen zullen alle maatregelen treffen die redelijkerwijs nodig zijn om (verdere) schending van de beveiligingsmaatregelen en eventuele schade te voorkomen of te beperken en zullen aan elkaar alle informatie verstrekken die zij nuttig of nodig achten.

10.3. Afhandeling datalek

De partijen beschikken over een plan voor de afhandeling van de datalekken en stellen dit op verzoek ter beschikking aan elkaar. Daarnaast houden ze een logboek bij van alle incidenten en maatregelen, die de desbetreffende partij kan inzien wanneer daarom gevraagd wordt.

10.4. Melding van klachten en verzoeken

De C-ITS Service Provider stelt AWW onmiddellijk in kennis van klachten, beschuldigingen of verzoeken met betrekking tot de verwerking van persoonsgegevens, ook indien deze afkomstig zijn van een toezichthoudende autoriteit. De C-ITS Service Provider verleent alle redelijke medewerking aan AWW in verband met dergelijke klachten of verzoeken, inclusief het verstrekken van relevante informatie en kopieën van de betrokken persoonsgegevens. Indien er klachten zijn inzake de C-ITS Service Provider, wordt deze daarvan in kennis gesteld.

Artikel 11: Standaardcontractbepalingen

niet van toepassing

Artikel 12: Relatie tussen de Partijen

12.1. Onafhankelijke Partijen

Deze Overeenkomst creëert geen partnerschap of andere formele zakelijke samenwerking tussen de Partijen. Beide Partijen blijven volledig onafhankelijk en handelen uit eigen naam. Geen van beide Partijen heeft de bevoegdheid om verplichtingen aan te gaan of beslissingen te nemen namens de andere Partij, tenzij dit uitdrukkelijk is vastgelegd in deze Overeenkomst.

12.2. Communicatie

In het kader van transparantie kunnen de Partijen communiceren dat gegevens worden uitgewisseld tussen AWW en de C-ITS Service Provider en desgevallend de bij de C-ITS Service Provider en bij AWW aangesloten derde partijen. De Partijen dienen ervoor te zorgen dat relevante informatie over de samenwerking, de use cases en de implicaties voor gegevensverwerking op een heldere en transparante manier beschikbaar is...

De C-ITS Service Provider verbindt zich ertoe op geen enkele wijze de indruk te wekken dat deze namens AWW communiceert of vertegenwoordigt.

12.3. Uitvoering van werkzaamheden

Beide Partijen voeren hun taken vrij en onafhankelijk uit, op basis van hun eigen kennis, expertise en planning. Dit gebeurt in overleg met de andere Partij waar nodig, maar er is geen sprake van een hiërarchische of gezagsrelatie tussen de Partijen, tenzij anders bepaald in deze Overeenkomst. De Partijen kunnen elkaar wel richtlijnen geven om de uitvoering van de Overeenkomst goed te laten verlopen.

Beide Partijen verbinden zich ertoe om deze overeenkomst te goeder trouw uit te voeren. Dit houdt in dat zij zich inzetten om hun verplichtingen eerlijk, transparant en volgens de gemeenschappelijke doelstellingen van de overeenkomst na te komen. In geval van onduidelijkheden of onvoorziene omstandigheden zullen de Partijen in onderling overleg redelijke en rechtvaardige oplossingen nastreven, met respect voor elkaars belangen.

Artikel 13. Aansprakelijkheid

13.1 AWW draagt geen enkele vorm van aansprakelijkheid voor schade die voortvloeit uit het niet delen of vertraagd delen van gegevens met de C-ITS Service Provider. AWW is ook niet aansprakelijk voor de correctheid van de inhoud van gegevens die gedeeld worden en draagt geen enkele vorm van aansprakelijkheid voor schade die voortvloeit uit de wijze waarop de C-ITS Service Provider of diens gebruiker(s) de gedeelde gegevens benutten. De gebruiker(s) van de gedeelde gegevens benutten deze op eigen risico en zijn te allen tijde verantwoordelijk voor correct en passend gebruik in overeenstemming met de regelgeving.

Dit omvat alle soorten schade, direct of indirect, ten gevolge van een verkeersongeval en andere, verlies van gegevens, onderbrekingen in de werkzaamheden, schade aan apparatuur, software of andere gegevens op de systemen van de C-ITS Service Provider of de gebruiker(s).

Deze uitsluiting van aansprakelijkheid geldt echter niet in geval van opzet, bedrog, of aansprakelijkheid op grond van dwingende wettelijke bepalingen, waaronder maar niet beperkt tot de Algemene Verordening Gegevensbescherming (AVG).

13.2 De C-ITS Service Provider staat er ten aanzien van AWW voor in dat enige aansprakelijkheidsbeperkingen tussen de C-ITS Service Provider en zijn gebruiker(s) met betrekking tot het benutten van de door AWW gedeelde gegevens doorwerken naar AWW, bij gebreke waaraan de C-ITS Service Provider hiervoor ten aanzien van AWW aansprakelijk zal zijn.

13.3. Elke Partij zal de andere Partij vrijwaren en schadeloosstellen voor alle directe en indirecte schade veroorzaakt door de niet of foutieve naleving van verbintenissen onder deze overeenkomst (met inbegrip van vorderingen van derden).

Wanneer een verhaal door derden wordt uitgeoefend vrijwaart elke aansprakelijke Partij de andere Partij. Elke Partij komt op eenvoudig verzoek van de andere Partij vrijwillig tussen in elk geschil dat zou worden gevoerd door derden met betrekking tot deze overeenkomst, ongeacht voor welke rechtbank, rechter en/of arbiter.

Artikel 14. Toepasselijk recht en geschillenbeslechting

Deze overeenkomst wordt beheerst door het Belgisch recht.

Alle geschillen die voortvloeien uit of verband houden met deze overeenkomst worden beslecht door de bevoegde Nederlandstalige rechtbank in Brussel.

Artikel 15. Inwerkingtreding

Deze overeenkomst treedt in werking op 29 augustus 2025.

Opgemaakt te Brussel, op 29 augustus 2025, in evenveel exemplaren als dat er partijen zijn.



Kathy Vandenmeersschant

[namens AWW]



[namens C-ITS DIENSTVERLENER]

Bijlage 1: Use cases

Use case (3): Waarschuwing Prioritair Voertuig

- Betrokken (categorieën van) persoonsgegevens:
 - Pseudoniem ID
 - Real-time verplaatsingsgegevens van prioritaire voertuigen en (indien gekend) type van prioritair voertuig
- Betrokkenen:
 - Bestuurders van hulpdienstvoertuigen in Vlaanderen en grensgebieden
- Business Context:
 - Weggebruikers worden gewaarschuwd voor aankomende hulpdienstvoertuigen
- Einddoel:
 - Verminder het aantal ongevallen met prioritaire voertuigen. De veiligheid van gebruikers van prioritaire voertuigen en andere weggebruikers wordt verhoogd door het bewustzijn te verhogen. Daarnaast kan de reistijd verkort worden door tijdige vorming van een reddingsstrook.
- Bijzonderheden:
 - Binnen deze overeenkomst is er voor deze use case enkel gegevensuitwisseling van C-ITS Service Provider naar AWW. De C-ITS Service Provider ontvangt de door AWW uitgestuurde waarschuwingen niet.
 - Dit is een use case vermeld onder artikel 8.3 d) met betrekking tot prioriteit- en toegangsrechten.

Use case (7): Waarschuwing Traag Hulpdienstvoertuig of Afschermend voertuig (met botsabsorbeerder)

- Betrokken (categorieën van) persoonsgegevens:
 - Pseudoniem ID
 - Real-time verplaatsingsgegevens van prioritaire voertuigen en (indien gekend) type van prioritair voertuig
 - Real-time verplaatsingsgegevens van voorsignalisatie- of afschermdende voertuigen, dienst- of werfvoertuigen tijdens interventies of werkzaamheden en type van voertuig
- Betrokkenen:
 - Bestuurders van hulpdienstvoertuigen in Vlaanderen en grensgebieden
 - Bestuurders van voorsignalisatie- of afschermdende voertuigen, dienst- of werfvoertuigen in Vlaanderen en grensgebieden
- Business Context:
 - Waarschuw de nabije weggebruiker dat een hulpdienstvoertuig, dienstvoertuig (of gelijkaardig) aanwezig is of manoeuvreert op een locatie, zodat deze zijn aandacht verhoogt en gedrag aanpast.
- Einddoel:
 - Informeer naderende weggebruikers over een mobiele werkzone of incidentlocatie waar zij dienstvoertuigen of hulpdiensten kunnen tegenkomen.
- Bijzonderheden:
 - Binnen deze overeenkomst is er voor deze use case enkel gegevensuitwisseling van C-ITS Service Provider naar AWW. De C-ITS Service Provider ontvangt de door AWW uitgestuurde waarschuwingen niet.
 - Dit is een use case vermeld onder artikel 8.3 d) met betrekking tot prioriteit- en toegangsrechten.

Use case (14): Tijd-tot-groen-informatie van intelligente verkeerslichten (iVRI)

- Betrokken (categorieën van) persoonsgegevens:
 - geen persoonsgegevens
- Betrokkenen:
 - geen
- Business Context:
 - Intelligente verkeerslichten delen gegevens met betrekking tot de status en timing van de verkeerslichten-regeling. Het informeren van de weggebruiker over de tijd-tot-groen.
- Einddoel:
 - Het efficiënter gebruik van de groen-fase bij een verkeerslicht, door het tijdig voorbereiden op het groen-worden van het licht.
 - Het duurzamer naderen van een verkeerslicht, door het vermijden van een stop bij nakend groen-worden van het licht.

Use case (15): Prioriteit bij intelligente verkeerslichten (iVRI) voor prioritaire voertuigen

- Betrokken (categorieën van) persoonsgegevens:
 - Pseudoniem ID
 - Real-time verplaatsingsgegevens van prioritaire voertuigen en (indien gekend) type van prioritair voertuig
 - Geschatte aankomsttijd bij het kruispunt en geplande oversteekbeweging van prioritaire voertuigen.
- Betrokkenen:
 - Bestuurders van prioritaire voertuigen in Vlaanderen en grensgebieden, in de buurt van intelligente verkeerslichten
- Business Context:
 - Prioritaire voertuigen kunnen prioriteit (groen) aanvragen aan intelligente verkeerslichten. Het verkeerslicht probeert daarop groen te geven, en het andere verkeer zo veel mogelijk te beperken.
- Einddoel:
 - Het oversteken van de lichten-geregelde kruispunten voor prioritaire voertuigen veiliger maken, door het aantal passages bij rood te verminderen.

- o Het verminderen van de verliestijd van prioritaire voertuigen door de verkeerslichten-regeling voor die voertuigen aan te passen ("absolute prioriteit").
- Bijzonderheden:
 - o Dit is een use case vermeld onder artikel 8.3 d) met betrekking tot prioriteit- en toegangsrechten.

Bijlage 2:

Methodes om de juistheid van de voertuigen en voertuigtypes te garanderen:

- Aantonen door: kopie van het inschrijvingsbewijs, kopie van het Europees certificaat van overeenstemming.
- Voor prioritair voertuig, bijkomend foto's waarop de nummerplaat en de kenmerken van het prioritair voertuig duidelijk zichtbaar zijn
- Controle voertuigtype via Kruispuntbank Voertuigen van FOD Mobiliteit & Vervoer
- Beleidsmatige controle a.d.h.v. aansluiting via track&trace provider, voor voertuigvloot met ingebouwde T&T. Beleidsmatige zekerheid van geconfigureerde voertuigtypes wordt voorzien.
- Andere methode, die voorafgaandelijk werd goedgekeurd door AWW

Bijlage 3: Standaardcontractbepalingen

niet van toepassing

Bijlage 4: Protocol

Bijlage 5:

Minimale voorwaarden voor aansluiting van de Specifieke Organisaties, met specifieke eisen voor rechtenbeheer, voertuigen en devices:

Beleid en maatregelen m.b.t. toegangsbeheer/autorisatie en beveiliging

C-ITS Service Provider dient het proces en beleid m.b.t. toekenning van rechten en autorisatie voor devices te beschrijven en ter goedkeuring voor te leggen aan AWW.

Beleid en maatregelen voor het verzekeren van koppeling tussen aanvragend device en voertuig waarvoor prioriteitsrechten werden toegekend

Minimale maatregelen moeten opgenomen worden in overeenkomsten van de C-ITS Service Provider met de Specifieke Organisatie. Toegelaten maatregelen zijn:

- Het vereisen van ofwel een fysische koppeling, ofwel een bluetooth-koppeling of gelijkwaardig, ...
- Ofwel akkoord/ondertekening van de gebruiker van een gedragscode of reglement voor het uitsluitend gebruik van het device in overeenkomstige wagen(type).
- Ofwel een andere maatregel, die voorafgaandelijk werd goedgekeurd door AWW.

Beleid activatie Use Cases

Volgende minimale maatregelen wordt opgenomen in overeenkomsten van de C-ITS Service Provider met Specifieke Organisaties, met betrekking tot wanneer de use cases geactiveerd worden. Op deze voorwaarden wordt weliswaar niet actief gemonitord. De Specifieke Organisatie dient zelf de naleving ervan op te volgen.

- Beleid activatie hulpdienst-prioriteit en/of –waarschuwing:
- enkel actief als voertuig prioritair rijdt Bij voorkeur, koppeling met blauw-knipperlicht-activatie.
- Beleid activatie dienstvoertuig waarschuwingen: enkel actief als het dienstvoertuig opdracht uitvoert. Bij voorkeur, koppeling met oranjegeel-knipperlicht-activatie.
- Beleid activatie aanvragen prioriteit voor openbaar vervoer: enkel indien actief voor dienst, en bij voorkeur enkel wanneer afstemming met rittenschema prioriteit noodzaakt.

Beleid en maatregelen om locatie-spoofing tegen te gaan:

Minimale maatregelen moeten door de C-ITS Service Provider en Specifieke Organisaties worden toegepast om spoofing tegen te gaan. Minimale oplossingen zijn:

- Gebruiksvoorwaarden vermelden dat het spoofen van locatie niet toegelaten is
- Geen "jailbroken device".
- Gebruik maken van functies op het platform om gesimuleerde positiegegevens te detecteren of te blokkeren.
- Bij detectie van bovenstaande wordt ofwel app-gebruik niet toelaten, ofwel gegevensuitwisseling met de Mobilidata Interchange productie-omgeving verhinderd