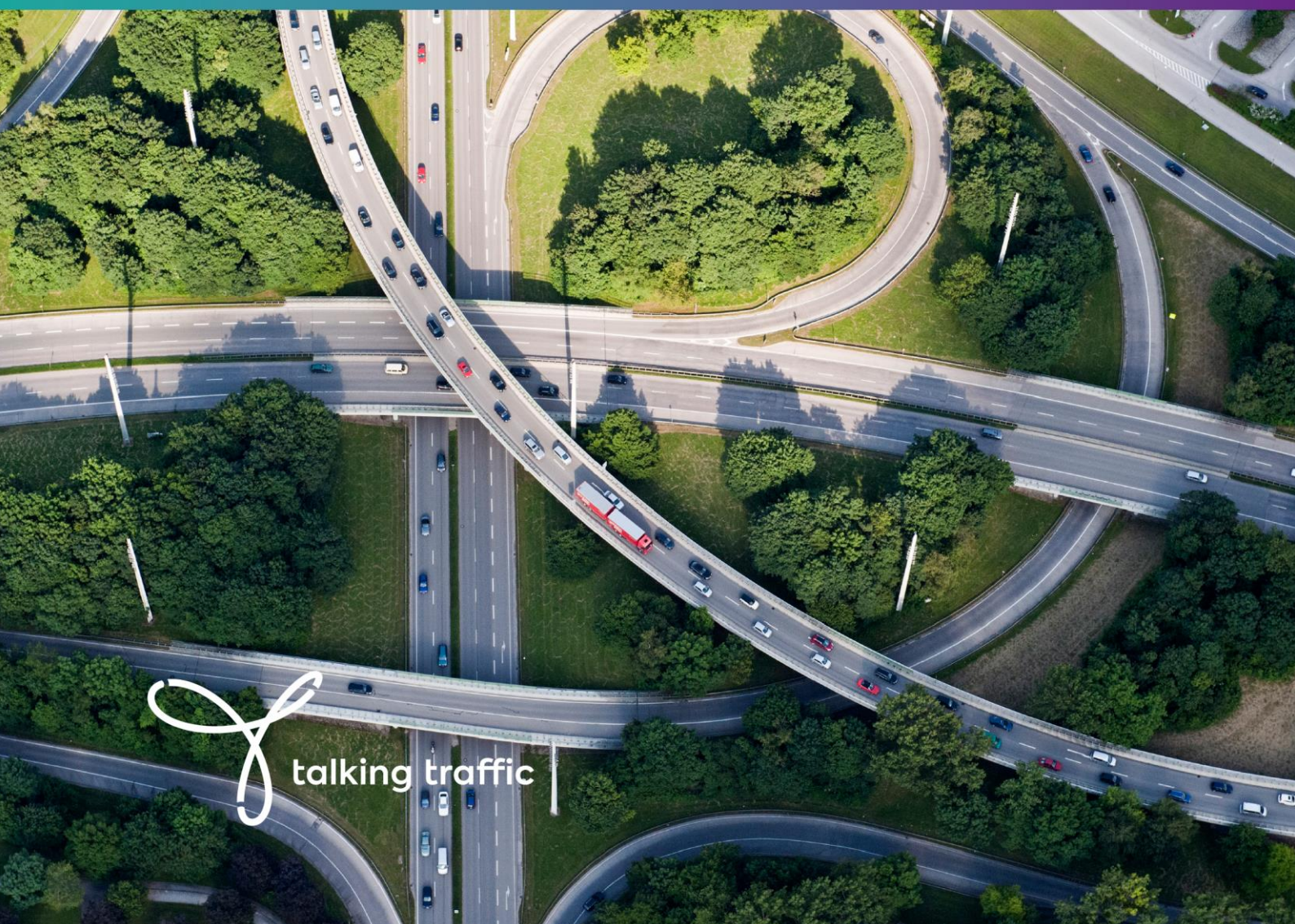


Rapport

KETENBREDE PRIVACY IMPACT ASSESSMENT DATAKETEN TALKING TRAFFIC



talking traffic

COLOFON

Titel:	Ketenbrede Privacy Impact Assessment Dataketen Talking Traffic
Opdrachtgever en eigenaar:	Ministerie van Infrastructuur en Waterstaat DG Mobiliteit, directie Mobiliteit en Gebieden
Met bijdragen van:	Privacy Company B.V.
Datum eerste versie	15 mei 2020
Datum tweede versie:	14 september 2022
Status rapport:	DEFINITIEF
Eerst versie van de PIA is uitgevoerd door DTV Consultants B.V. PBLQ op 15 mei 2020. Tweede versie van de PIA is uitgevoerd door Privacy Company B.V. op 14 september 2022	

1	INLEIDING	4
2	BESCHRIJVING DATAKETEN TALKING TRAFFIC	7
2.1	DE IVRI IN DE DATAKETEN	13
2.1.1	Functionaliteiten van de iVRI - Use Cases	14
2.1.2	De iVRI standaarden	17
2.1.3	Technische architectuur met internationaal gestandaardiseerde koppelvlakken	18
2.2	MEER WETEN?	23
3	DE IVRI EN PRIVACY	25
3.1	DATA VAN EN NAAR IVRI'S IN RELATIE TOT PRIVACY	25
3.1.1	Data van en naar iVRI's	25
3.1.2	Het gebruik van iVRI-data per schakel in de dataketen	29
3.2	VERWERKINGSVERANTWOORDELIJKE EN VERWERKER	31
3.2.1	Verwerkingsverantwoordelijken	32
3.2.2	Verwerkers	33
3.3	GRONDSLAG VERWERKING PERSOONSgegevens	35
3.3.1	Grondslag wegbeheerders	35
3.3.2	Grondslag service providers (Cluster 3)	36
3.4	PROPORTIONALITEIT EN SUBSIDIARITEIT	39
3.5	VERANTWOORDELIJKHEDEN PARTIJEN TALKING TRAFFIC KETEN	41
3.6	Risico's en te treffen maatregelen	46



1 INLEIDING

Om Smart Mobility in publiek-private samenwerking te faciliteren, zijn het Ministerie van Infrastructuur en Waterstaat met Rijkswaterstaat, zo'n 80 decentrale overheden en 20 (inter)nationale bedrijven uit de verkeersindustrie, telecom- en internetsector, dienstverlening en automotive sector het Innovatiepartnerschap Talking Traffic gestart. Gezien de toenemende drukte met alle negatieve gevolgen van dien voor weggebruikers, inwoners en bedrijven is het doel van dit Innovatiepartnerschap het verbeteren van de doorstroming, de verkeersveiligheid en de bereikbaarheid in en rond steden in Nederland.

Het middel om het doel te bereiken is het frequent versturen van complete en actuele persoonlijke informatie zodat weggebruikers slimmere rij- en routekeuzen kunnen maken en wegbeheerders hun wettelijke taken en verantwoordelijkheden effectiever kunnen invullen. Op een instrumenteel niveau betekent dit het beschikbaar maken en standaardiseren van elektronische berichten, de voorwaarden waaronder die berichten beschikbaar komen en gebruikt worden.

Die elektronische berichtenuitwisseling gebeurde al in het private domein sinds begin jaren '90 van de vorige eeuw met de opkomst van TomTom en andere navigatiedienstverleners. Eerst alleen als routeplanners, maar gaandeweg meer als online rijtaakondersteuning en reis-assistent. Gezien de toenemende automatiseringsfuncties ('advanced driver assistance systems ADAS') gericht op comfort, veiligheid en energieverbruik zet die trend zich voort in het voertuig.

Wegbeheerders hebben hier vanaf ca. 2010 gebruik van gemaakt met de inrichting van de Nationale Databank Wegverkeersgegevens (NDW): het inkopen van private data t.b.v. reistijden en intensiteiten als indicatoren van het weggebruik t.b.v. hun eigen, publieke verkeersmanagement. Tegen die achtergrond is het Innovatiepartnerschap gestart in 2016, als 5-jarige impuls voor de ontwikkeling van nieuwe functionaliteiten in apps en navigatiesystemen en het aanjagen van de commerciële beschikbaarheid ervan, als ook een vorm van publiek-publieke (IenW, RWS, provincies, gemeenten) en publiek-private samenwerking op basis van uniforme vereisten, governance structuur en contractuele overeenkomsten.

Dit proces verliep tegen de achtergrond van elkaar in rap tempo opvolgende ontwikkelingen in de internationale automobiellindustrie, de intensivering in internetgebruik door consumenten, bedrijven en overheden, maar ook de voortgaande verstedelijking, druk op fysieke ruimte, klimaat- en leefbaarheidsproblematiek. Naast beleidsmakers hebben wegbeheerders een belangrijke wettelijke taak in het beschikbaar stellen en houden van weginfrastructuur en het reguleren van veilig, duurzaam en verantwoord gebruik van die infrastructuur volgens geldende wet- en regelgeving.

In het inhoudelijke pakket van 6 groepen gebruikstoepassingen dat binnen het Innovatiepartnerschap is ontwikkeld, spreken de 3 groepen van toepassingen met verkeerslichten het meest in het oog. Niet onbegrijpelijk, omdat hier de geautomatiseerde elektronische berichtenuitwisseling de grootste verandering aanbrengt in de bestaande werkwijze, techniek en verantwoordelijkheden, zowel aan publieke zijde als in de private sector. Een goed gestructureerde governance, uniforme technische eisen en standaarden en contractmanagement zijn daarom van belang om alle spelers effectief en verantwoord te laten opereren binnen wettelijke kaders en ten gunste van de samenleving en individuele weggebruikers (in alle modaliteiten).

De nieuwe generatie verkeerslichten, de intelligente verkeersregelininstallaties oftewel iVRI's, zijn onderdeel van een dataketen en sturen data naar en ontvangen data vanuit deze keten. In deze dataketen wordt ook publieke data over wegwerkzaamheden, parkeren, verkeersborden, incidenten, snelheden en verkeersintensiteiten beschikbaar gesteld, verwerkt en gebruikt. Private partijen, zoals cloud providers en service providers, gebruiken de publieke data, om hun gebruikers adequaat te kunnen informeren. Voor de regeling van verkeerslichten op kruispunten in en om de stad produceren en leveren deze private partijen verplaatsingsdata. Dit is op basis van de data van weggebruikers die apps gebruiken op hun smartphone. Ook professionele weggebruikers als openbaar vervoer, nood- en hulpdiensten en vrachtverkeer maken gebruik van de mix van publieke en private data.

Een dergelijke samengestelde publiek private dataketen heeft in de planvorming, aanbesteding en contracten, maar ook tijdens de uitvoering veel en gerichte aandacht gegeven aan randvoorwaardelijke aspecten als verantwoordelijkheidsverdeling, privacy en security. De voorliggende rapportage beschrijft het technisch opereren van deze keten, waarin:

- de gehele dataketen met betrekking tot privacy volledig is beschreven; de beschrijving ten behoeve van cybersecurity is een apart document;
- de belangrijkste technische handelingen in de dataketen ten aanzien van privacy zijn per schakel geïdentificeerd;
- beheersmaatregelen zijn benoemd om de geïdentificeerde risico's ten aanzien van privacy in de dataketen te beheersen.

Deze rapportage is nadrukkelijk gericht op de dataketen en risico's en beheersmaatregelen op het niveau van de dataketen. De rapportage komt nadrukkelijk niet in de plaats van analyses en beheersmaatregelen die de verantwoordelijkheid zijn van de afzonderlijke publieke en private organisaties die deelnemen in de dataketen. Wel wordt apart aandacht besteed aan de rol en verantwoordelijkheid van de individuele wegbeheerder en diens handelingsperspectief met betrekking tot privacy (en security, maar dat is een apart document weergegeven).

Doel rapportage

Het doel van deze rapportage is het bieden van:

1. Een beknopte, toegankelijke beschrijving van de Talking Traffic dataketen op het niveau van de keten vanuit het oogpunt van privacy, zodanig dat privacy-functionarissen van vooral overheden, maar ook van bedrijven, vanuit hun eigen expertise begrijpen wat deze dataketen inhoudt, hoe deze functioneert en welke data wordt uitgewisseld;
2. Een systematische, gestructureerde analyse van risicovolle onderdelen in deze dataketen en de maatregelen op het niveau van de keten in relatie tot privacy;
3. Praktische beheersmaatregelen op het niveau van de keten om de geïdentificeerde risicovolle onderdelen in deze dataketen te beheersen;
4. Individueel handelingsperspectief aan een wegbeheerder om de eigen verantwoordelijkheid de juiste vorm en inhoud te geven.

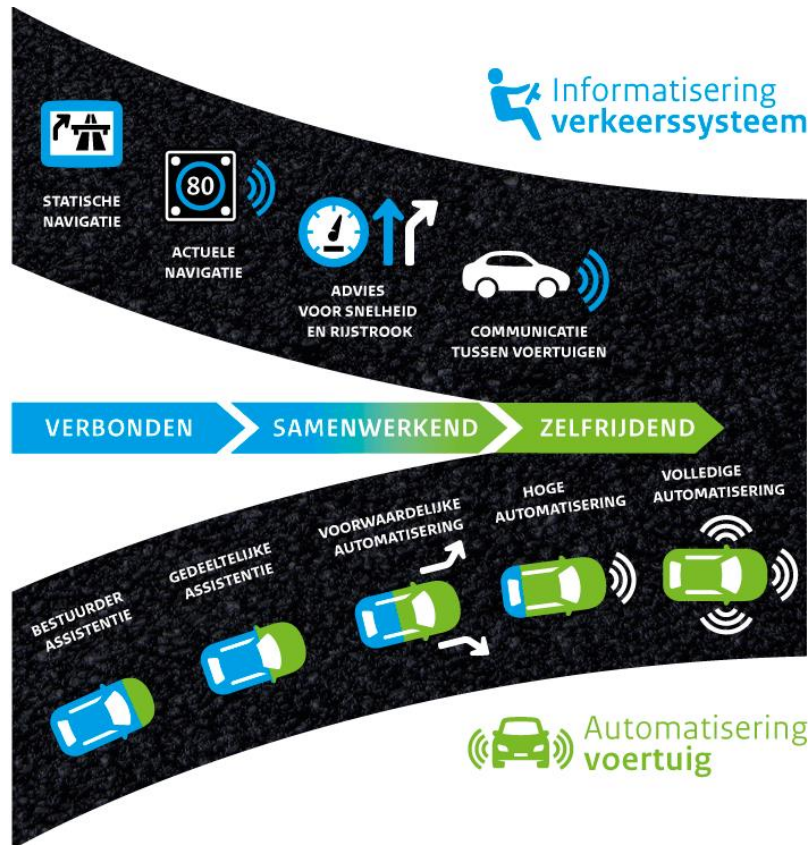
Leeswijzer

Dit document begint met een beschrijving van de dataketen van Talking Traffic in hoofdstuk 2. Daarna worden de grondslag, proportionaliteit en beheersingsinstrumenten voor het onderdeel Privacy in hoofdstuk 3 beschreven. In de bijlagen is een top 5 risicoparagraaf met beheersmaatregelen weergegeven, als ook de metingen van resultaten in het gebruik van iVRI's.

Beschrijving dataketen Talking Traffic

2 BESCHRIJVING DATAKETEN TALKING TRAFFIC

Voertuigen worden onderdeel van het Internet of Things. Voertuigen nemen steeds meer rijtaken van de bestuurder over, kunnen communiceren met andere voertuigen en met verkeerssystemen zoals verkeerslichten. De ontwikkelingen zijn onderdeel van het bredere Smart Mobility en vinden plaats langs twee paden (zie Figuur 1) die, als ze eenmaal samenkomen in de verdere toekomst, leiden tot een aanzienlijk of zelfs volledig zelfrijdend en/of zelfsturend connected verkeerssysteem.



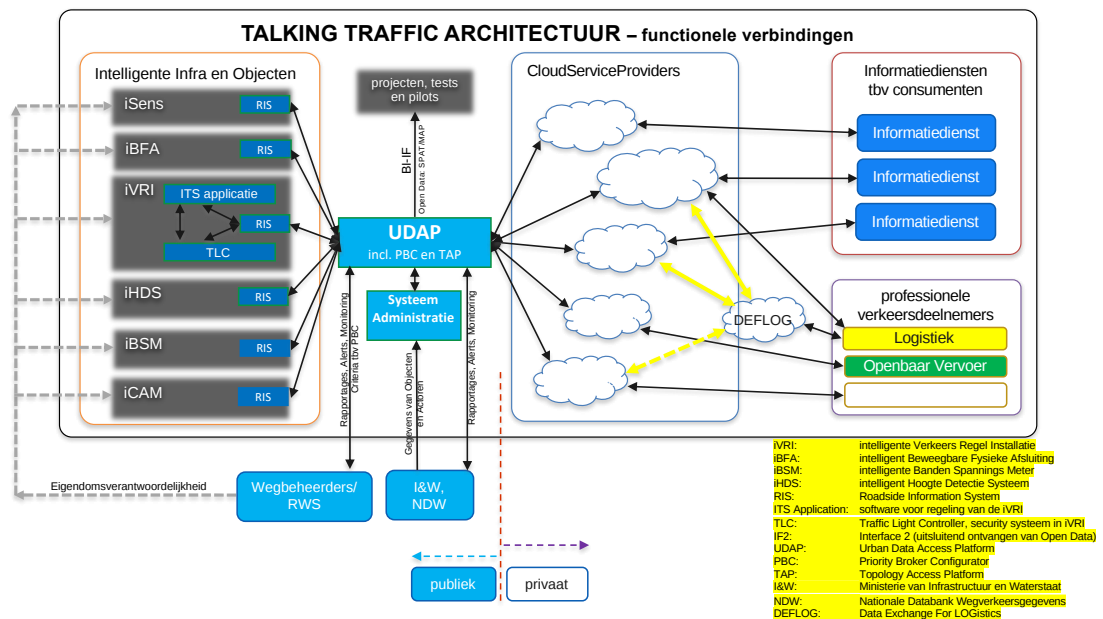
Figuur 1 Twee belangrijke ontwikkelpaden verkeerssysteem

Om Smart Mobility in publiek private samenwerking te faciliteren, zijn het Ministerie van Infrastructuur en Waterstaat met Rijkswaterstaat, zo'n 60 decentrale overheden en 20 (inter)nationale bedrijven uit de verkeersindustrie, telecom- en internetsector en dienstverlening- en automotive sector het Innovatiepartnerschap Talking Traffic gestart. Samen werken zij aan de ontwikkeling van innovatieve verkeerstoepassingen die bijdragen aan een betere bereikbaarheid, meer reiscomfort, minder ongevallen en meer vergroening van onze mobiliteit.

Drie clusters binnen Talking Traffic

Het Innovatiepartnerschap Talking Traffic kent een in drie Clusters opgedeelde dataketen (zie Figuur 2), waarbinnen partners samenwerken aan het versnellen van deze ontwikkeling. De indeling in Clusters is gekozen zodat de overheidsinvesteringen beter gericht kunnen worden,

markdominantie van een enkele partij kan worden voorkomen en de taken, activiteiten en verantwoordelijkheden in de keten scherp vastgelegd kunnen worden. Dat geeft overzicht over de functies in de keten en schept duidelijkheid over de verantwoordelijkheden van individuele organisaties en de onderlinge leveringsafspraken ten aanzien van datalevering en kwaliteit. Tussen deze drie Clusters stromen gegevens: van Cluster 1 via Cluster 2 naar Cluster 3 én andersom.



Figuur 2 Het Innovatiepartnerschap Talking Traffic op basis van de opgeleverde documentatie¹

Cluster 1 ("de iVRI-leveranciers") ontsluit verkeerslichtgegevens en maakt gebruik van gegevens vanuit de weggebruiker. Met deze informatie kan de iVRI de weggebruiker beter informeren én kan de iVRI tegelijkertijd slimmer worden geregeld. De individuele wegbeheer is verantwoordelijk voor aanschaf en inzet van een iVRI, en zal daartoe een (of enkele) partij(en) uit Cluster 1 contracteren. Een iVRI bestaat uit drie typen onderdelen: de TLC (Traffic Light Controller) die als het ware het veiligheidsnet voor het regelsysteem van de iVRI vormt, een RIS (Roadside ITS Station) die verantwoordelijk is voor lokatiegegevens binnen de de iVRI en de communicatie met de buitenwereld, en tenslotte een of enkele ITS-App's die de intelligente regeling van de iVRI verzorgt/verzorgen. Deze onderdelen communiceren met elkaar en de RIS communiceert met onder andere UDAP (Urban Data Access Platform). Elke iVRI maakt contact met UDAP en elke Cluster 2 partij maakt contact met UDAP. UDAP vormt een het centrale doorgeefluik tussen de juiste iVRI (of een ander intelligent infrastructureel object) in Cluster 1 en de juiste cloud provider in Cluster 2. De UDAP beheert ook de database van de PBC (Priority Broker Configurator). De wegbeheerders geven in de PBC aan welke prioriteitsregels voor een iVRI gelden. De cloud providers ontvangen een kopie van deze database en gebruiken die om het statische voertuigtype (vehicle role) te vertalen naar een dynamische prioriteitsclassificatie.

¹ Zie verder URL: <https://www.talking-traffic.com/nl/partner-worden-bij-talking-traffic/clusters-en-expertise>

De cloud providers in Cluster 2 krijgen pas na certificering een aansluiting op UDAP. Zij hebben ondermeer tot taak om voor de bij hen aangesloten verkeersdeelnemers die gerechtigd zijn om prioriteit aan te vragen, prioriteitsverzoeken aan te maken en deze via UDAP naar de juiste iVRI te sturen. Daarnaast hebben de cloud providers in Cluster 2 ook de mogelijkheid om data uit een reeks van verschillende bronnen te verrijken met andere datastromen en deze om te zetten in op maat gemaakte real-time beschikbare datasets en informatie. Daarvoor kunnen de clouddiensten putten uit zowel publieke als private bronnen. Naast data uit iVRI's gaat het bijvoorbeeld over route-informatie en op basis daarvan verwachte reistijden van weggebruikers, wegwerkzaamheden, ongevallen en actuele parkeerdata.

Tot slot wordt door elk van de service providers in Cluster 3 de informatie ontsloten aan een breed scala van weggebruikers, via bijvoorbeeld smartphones en navigatiesystemen. Hierdoor worden zoveel mogelijk weggebruikers voorzien van informatiediensten, ongeacht het merk, type of leeftijd van hun vervoermiddel. Tegelijkertijd zorgen de partijen in Cluster 3 er voor dat relevante informatie (zoals locatie, rijrichting, ETA, manoeuvre) uit de voertuigen van hun gebruikers, via Cluster 2 en UDAP, terechtkomt bij de juiste iVRI's in Cluster 1, zodat deze op basis van die gegevens efficiënter kunnen regelen.

NB: in de overdracht van dergelijke berichten zijn technische en organisatorische maatregelen genomen die voorkomen dat wegbeheerders inzicht krijgen in persoonlijke kenmerken of dat bedrijven toegang krijgen tot persoonlijke kenmerken waartoe zij niet gerechtigd zijn. De wijze waarop dit gebeurd is beschreven in paragrafen 2 en 3.

In 2021 zijn er meer dienstverleners op UDAP aangesloten dan voorheen het geval was (toen de naam van deze "brug" tussen Cluster 2 en Cluster 1 nog "TLEX" luidde). Tegelijkertijd hebben de twee nieuwe cloud providers in Cluster 2 ook een informatiedienst ("Cluster 3") toegevoegd aan hun dienstverlening. Deze beide nieuwe cloud providers in Cluster 2 zijn eveneens leverancier van apparatuur en diensten in Cluster 1.

Geofences: een belangrijk technisch principe

Aan de berichtenuitwisseling binnen Talking Traffic ligt een elementair technisch principe ten grondslag: **de geofence techniek**. Dit is een virtueel gemarkeerd gebied op een digitale kaart. Dat kan een lijn zijn, een polygon of een cirkel. Voor het doel van deze ketenbrede PIA is het belangrijk om te beseffen dat een groot gebied (bijv. regio Oost Nederland of Amsterdam) op die manier digitaal is onderverdeeld in vele deelgebieden en deeltrajecten. Voor kruispunt toepassingen zijn dat virtuele gefixeerde gebiedsmarkeringen. Voor andere toepassingen, bijvoorbeeld een pechgeval op de rijbaan, zijn dat tijdelijke virtuele markeringen die verdwijnen als de aanleiding verdwijnt (pechgeval is weggesleept).

Deze digitale markeringen van grotere of kleine gebieden en trajecten, deels gefixeerd, deels dynamisch, zijn relevant voor weggebruikers, de dienstverleners en wegbeheerders:

- Weggebruikers: worden in dat deelgebied op maat bediend, want krijgen bij het passeren van die digitale grens een bericht dat op dat moment voor hen relevant en toepasbaar is. Bijv. omdat zij een kruispunt met een verkeerslicht naderen en dan hun snelheid kunnen aanpassen.

- Dienstverleners: zenden uitsluitend die berichten uit die op dat moment, op die locatie, voor desbetreffende weggebruiker relevant en toepasbaar zijn. Bijvoorbeeld 'u nadert een kruispunt en het verkeerslicht staat voor u op rood'.
- Wegbeheerders: ontvangen door gecontracteerde iVRI-leverancier(s) slechts een tijdelijke pseudo-identiteit vanuit het private domein over het soort voertuig (fiets, auto, bus, ambulance, vrachtwagen) dat een kruising nadert, de actuele locatie van het voertuig en -indien het voertuig prioriteit gerechtigd is- tevens de ETA (Expected Time of Arrival) op de stopstreep en de aan de PBC (Priority Broker Configurator) ontleende prioriteitsklasse van dat voertuig, die voor die regeling op dat kruispunt relevant is. Bijvoorbeeld 'over 80 seconden arriveert een vrachtauto met prioriteitsklasse 7 op de stopstreep bij signaalgroep 3 van dit kruispunt'. Na vertrek uit dat gemarkeerde gebied of passeren van die stopstreep, verdwijnt die pseudo-identiteit en wordt bij naderen van een volgende iVRI een nieuwe, wederom tijdelijke, pseudo-identiteit aangemaakt.

In het onderdeel "TAP" (Topology Access Portal) van UDAP is voor iedere iVRI een topologisch bestand verzameld, dat door desbetreffende iVRI als MAP-bestand ten behoeve van naderende voertuigen wordt verzonden. In zo'n digitaal topologische bestand zijn alle relevante geografische gegevens met betrekking tot de iVRI opgenomen, waaronder die over de voorsorteervakken, markeringen en locaties van de lichten, binnen een afstand van doorgaans maximaal 300 meter van de stopstreep. Bij het aanvragen van prioriteit voor specifieke doelgroepen zoals voor hulpdiensten, OV bussen en zware vrachtwagens kan aan de hand van de gegevens in zo'n MAP-bestand het voertuig diens komst aankondigen tot maximaal 5 minuten voor het bereiken van de stopstreep.

Rollen en verantwoordelijkheden publieke domein

In Figuur 2 is een grens te trekken als het gaat om de directe publieke verantwoordelijkheid van individuele wegbeheerders en de verantwoordelijkheid van het Ministerie van Infrastructuur en Waterstaat.

Wegbeheerder als zelfstandig verwerkingsverantwoordelijke

Een weg wordt beheerd en onderhouden door een wegbeheerder. Uit de Wegenverkeerswet volgt de wettelijke taak voor de wegbeheerder. Uitgangspunt is de vlotte doorstroming van het verkeer. De wegbeheerder is verantwoordelijk om de beschikbaarheid en het veilig gebruik van de fysieke weginfrastructuur te borgen en beheren met gebruik van uiteenlopende middelen en instrumenten. Dit zijn fysieke en digitale middelen. Bij fysieke middelen moet gedacht worden aan borden, informatiepanelen, inductielussen, camera's, verkeerslichten. Bij digitaal herkenbare middelen moet gedacht worden aan detectie en operatie waaronder regelscenario's, verkeersintensiteiten, TMC feeds, databases van verkeersborden, Nationaal Wegenbestand, etc. Het extern beschikbaar maken van uiteenlopende digitale instrumenten en datasoorten voor gebruik in het private domein is een praktijk die vanaf circa 2010 is ontstaan en in de toekomst verder zal groeien. Het Innovatiepartnerschap Talking Traffic past in die ontwikkeling.

iVRI-Leverancier als verwerker

Cluster 1 bestaat uit de leveranciers van de (onderdelen van de) verkeersregelininstallaties die door wegbeheerders worden gecontracteerd. In die hoedanigheid is zo'n leverancier verantwoordelijk voor de levering van een installaties en het onderhoud ervan. De leverancier

doet dit *in opdracht van* de wegbeheerder(s). De leverancier is daarom verwerker van de wegbeheerder. Per wegbeheerder kunnen dat meerdere leveranciers zijn die verschillende installaties leveren en beheren. De iVRI standaarden maken het ook mogelijk dat de verschillende componenten van een iVRI (TLC, RIS en ITS-App) door verschillende leveranciers geleverd worden. De iVRI's verzenden data die verder in de keten gebruikt wordt: de MAP-data (digitale topologische bestanden) en SPaT-data (Signal Phase and Timing), een constante stroom data met de actuele status en regelcycli van alle signaalgroepen op het kruispunt.

De data die afkomstig is uit een iVRI wordt in opdracht van de wegbeheerder geleverd aan UDAP. Op dezelfde wijze en onder dezelfde verantwoordelijkheid van die wegbeheerder ontvangt deze iVRI bewerkte, gepseudononimiseerde data vanuit UDAP om de regelcycli te kunnen afstemmen op de verkeersstromen op het kruispunt of een reeks van kruispunten op het fysieke netwerk. UDAP vormt daarbij de "brug" tussen de partijen in Cluster 1 en die in Cluster 2.

Meerdere wegbeheerders zijn opdrachtgever en deelnemer in NDW, de Nationale Databank Wegverkeer die verkeersdata uit publieke systemen als Open Data beschikbaar stelt aan de private sector. (onderaan Figuur 2)

Public trafficmanagement en data systeem

Het Public trafficmanagement systeem en data systeem is een volledig publieke organisatie. Dit betreft de voorzieningen van Rijkswaterstaat. In dit systeem wordt publieke data voor verkeersmanagement gebruikt en extern beschikbaar gesteld middels datafeeds, al of niet via NDW.

Het Ministerie van Infrastructuur en Waterstaat

Het Ministerie van Infrastructuur en Waterstaat (verder lenW) is als systeemverantwoordelijke van UDAP voor alle verkeer in Nederland de initiator en regisseur voor de publiek-private samenwerking, de werking van de dataketen middels UDAP, het borgen van de gezamenlijke governance, de verkeersveiligheidsaspecten van nieuwe diensten en functionaliteiten. Dit onverlet de afzonderlijke verantwoordelijkheden van overheden en wegbeheerders in hun eigen beheergebied respectievelijk de verantwoordelijkheden van private partijen onder geldende Nederlandse wet- en regelgeving.

lenW is als Aanbestedende dienst verantwoordelijk is voor het toelaten van zowel private als publieke partijen tot UDAP. Zo moeten de private partijen onder meer voldoen aan de landelijke standaarden welke door lenW in beheer zijn gebracht bij kennisplatform CROW. De private partijen worden voor het aansluiten op UDAP gecontroleerd of zij voldoen aan de landelijke iVRI-standaarden. Verder houdt lenW actief toezicht op de naleving van de overeenkomsten en standaarden en kan partijen afsluiten als ze de voorwaarden niet naleven. Daarnaast behoudt lenW de controle over UDAP doordat zij pas wegbeheerders aansluit op UDAP indien zij een verwerkersovereenkomst met haar iVRI-leverancier heeft gesloten. Indien er geen actuele en geldende verwerkersovereenkomst door de wegbeheerder met haar ITS-, TLC- en/of RIS-leverancier is gesloten, zal (of zullen) de desbetreffende iVRI-installatie(s) niet tot UDAP worden toegelaten. Op deze wijze houdt lenW actief toezicht op zowel publieke als private partijen die gebruik (willen) maken van UDAP en het uitwisselen van gegevens tussen deze partijen.

De financiële inspanning die voortvloeit uit de aanbesteding betreft nadrukkelijk co-investeringen om ontwikkeling en levering aan derden (weggebruikers, wegbeheerders, bijzondere doelgroepen) te bevorderen. Er worden geen data, producten of diensten aan IenW zelf geleverd.

IenW heeft vanuit de overeenkomsten de verantwoordelijkheid voor het uitwisselingsmechanisme UDAP. Deze functie is een dienstencontract voor data-uitwisseling onder publieke opdracht en toezicht, dat is gesloten met de private organisatie Monotch², op basis van het resultaat van de daarvoor uitgevoerde Europese aanbesteding.

UDAP regelt de uitwisseling van data tussen iVRI's (formeel in beheer van de wegbeheerders) en de weggebruikers (via de partijen in de Clusters 2 en 3). Hierbij kan onderscheid gemaakt worden tussen twee verantwoordelijkheden, gelet op het leveren van een dienst onder publieke regie en verantwoordelijkheid bestaande uit twee activiteiten:

- Ontvangen van verkeerslichtdata en topologische data uit het publieke domein en het onder voorwaarden doorgeven hiervan aan private afnemers tegen gelijke voorwaarden; en
- Ontvangen van geanonimiseerde data vanuit cloud providers en deze doorgeven aan de juiste iVRI.

Gelet op de verantwoordelijkheid voor het beheer van UDAP, de besluitvorming of een private partij dan wel wegbeheerder wel of niet wordt aangesloten op UDAP, en het houden van toezicht op het uitwisselen van de data middels UDAP tussen de wegbeheerders enerzijds en de Cluster 2 en 3 anderszijds, zorgt ervoor dat voor zover er persoonsgegevens middels UDAP worden uitgewisseld IenW voor de verwerking van persoonsgegevens middels UDAP zelfstandig verwerkingsverantwoordelijke is. Zij bepaalt immers hoofdzakelijk het doel en de middelen van de verwerking.

Rollen en verantwoordelijkheden van bedrijven

Service providers als zelfstandige verantwoordelijke

Partijen in Cluster 3, de service providers, leveren individuele diensten aan hun klanten, zoals apps die helpen om de optimale route te vinden of apps waarmee prioriteitsrechtige voertuigen prioriteit aan kunnen vragen. Deze partijen maken gebruik van klantdata voor het leveren van een optimale dienst en geven via UDAP klantdata door aan de iVRI's van de wegbeheerders. Voor deze verwerking, die plaatsvindt voor eigen doeleinden van de service provider, zijn de service providers zelfstandig verwerkingsverantwoordelijke, aangezien zij de doelen en middelen van de verwerking bepalen.

Cloud providers als verwerker

Binnen Cluster 2 zijn er twee groepen dienstverleners (cloud providers):

De ene groep heeft de dienstverlening binnen de Clusters 2 en 3 verregaand geïntegreerd waardoor deze functioneel en juridisch niet meer tussen beide Clusters te onderscheiden is. Bij de andere groep is sprake van een duidelijk afgescheiden eenheid in Cluster 2, waar verschillende partijen uit Cluster 3 op kunnen aansluiten. Deze groep cloud providers houdt zich bij de communicatie met partijen in Cluster 3 aan het formaat van de CAM, SRM en SSM

² <https://www.talking-traffic.com/nl/urban-data-access-platform>

berichten en beperkt zich tot het doorgeven van die berichten. Zie Bijlage 2 voor een technische analyse per aanbieder in Cluster 2. De bewerking en doorgifte van data afkomstig van een partij uit Cluster 3 door een partij in Cluster 2 is hoe dan ook begrensd door de gebruikstoestemming die de partij uit Cluster 3 heeft verkregen van diens klanten.

In de volgende paragrafen worden deze rollen en verantwoordelijkheden beschreven naar de technische vertaling en betekenis voor data, verwerking en doorgifte. In paragraaf 3.5 is beschreven op welke wijze de governance, toezicht en controle is ingericht zodat ook duidelijk wordt op welke wijze de rolvastheid en verwerking in de keten is geborgd.

2.1 DE IVRI IN DE DATAKETEN

Doelen

Het voornaamste doel van de 3 groepen iVRI toepassingen binnen het Innovatiepartnerschap is gericht op het bevorderen dat verkeerslichten beter kunnen functioneren, zodat de verkeersafwikkeling op kruispunten efficiënter kan worden uitgevoerd. De verkeersintensiteit in en rond steden neemt toe, de beleidsdoelen die wegbeheerders dienen in te vullen zijn een veelvoud: doorstroming, bereikbaarheid, verkeersveiligheid, leefbaarheid, duurzaamheid, economische vitaliteit dienen allemaal zoveel als mogelijk bevorderd te worden. En dan met rekenschap van de verschillende gedragingen van verkeersdeelnemers (lopen, fietsen, personenauto's, OV, vrachtwagens, nood en hulpdiensten) met elk hun eigen karakteristieken, noodzaken en beperkingen waarbij politiek-bestuurlijke prioriteiten regelmatig andere accenten vergen in het accommoderen van de ene groep boven de andere (bijv. meer voorrang voor fietsers boven personenauto's) en het gebied zich ook blijft ontwikkelen en veranderen (denk aan nieuwe woonwijken en bedrijfsterreinen en/of kantoorlocaties). Binnen dat speelveld van doelen, belangen en veranderingen is de verkeersafwikkeling op kruispunten een belangrijke factor in het stedelijk weefsel en tegelijk zowel meetinstrument als regulator, die schaarse tijd en ruimte verdeelt en voortdurend rekening moet houden met het actuele verkeersaanbod (richting, route, snelheid, soort), pieken (spitsen uiteraard) en verdeling van de beschikbare fysieke en regelruimte. Aan de bestaande detectie via inductielussen en regelingen die daarop zijn gebaseerd, wordt nu de mogelijkheid toegevoegd om verkeerslichten fijnmaziger te regelen doordat meer en beter inzicht ontstaat in het actuele verkeersaanbod in al zijn diversiteit. En om dit op termijn goedkoper en effectiever te kunnen doen.

Daarin spelen minstens 3 factoren een rol:

- Onderzoek van DTV in 2014 bracht aan het licht dat 50% van de Nederlandse wegbeheerders nooit of hooguit eens per vijf jaar **de regelingen in verkeerslichten aanpast** aan gewijzigde omstandigheden. De jaarlijkse maatschappelijke kosten in Nederland werden ingeschat op € 90 miljoen. In de periode vanaf midden jaren '90 van de vorige eeuw heeft het Ministerie hierop herhaaldelijk een forse financiële en organisatorische inspanning gedaan met inzet van een zgn. Groene Golf-team. De kosten die het Ministerie hiervoor heeft gemaakt beliepen ca. € 20 miljoen. Dergelijke tijdelijke financiële impulsen vanuit het Rijk in lokale en regionale kerntaken zijn echter niet houdbaar gebleken.
- De **congestie** in het stedelijk gebied krijgt relatief gezien minder aandacht dan congestie op snelwegen. Toch laten jaarlijkse metingen van de totale voertuigverliesuren in gemeenten zien, dat op het stedelijk wegennet in Nederland de congestie in voertuigverliesuren gelijk of groter is dan die op snelwegen. De jaarlijkse metingen van o.a. TomTom laten zien welke

steden daarin de kroon spannen. Met uiteraard de nodige gevolgen voor economische aantrekkelijkheid van deze steden, de uitstoot en leefbaarheid voor omwonenden en klimaatdoelstellingen die inmiddels een steeds grotere prioriteit krijgen.

- De wijze van **detectie** via inductielussen is kwetsbaar en kostbaar. Vorst en regen, beschadigingen door zwaar verkeer zorgen voor uitval en intensieve beheerinspanningen en storingsopvolging vanuit de overheden. Daarbij kan de hoeveelheid inductielussen per kruispunt oplopen tot 70 stuks waarbij jaarlijks per lus ca. € 1000,- gemoeid is met beheer, onderhoud en storingsopvolging.

Bij de uitrol van iVRI's is duidelijk geworden dat de **Nood- en Hulpdiensten en Veiligheidsregio's** ook belangrijke baathebbers zijn. Op weg naar een calamiteit en met gebruik van sirene en zwaailicht gaat het per jaar ca. 240 keer mis op een geregeld kruispunt omdat deze voertuigen door rood licht moeten rijden. Andere weggebruikers herkennen deze aankomende voertuigen niet of pas te laat. Met als gevolg een extra ongeval op een kruispunt en een later aankomsttijdstip bij het incident of ongeval dat de eigenlijke reden voor de oproep van de ambulance, brandweer of politie was.

Er zijn dan ook meerdere goede redenen om te streven naar betere, aanvullende en kosten-efficiëntere manieren van voertuigdetectie en het regelen van verkeerslichten. Dat streven heeft geresulteerd in iVRI's, welke onder strikte voorwaarden onderdeel kunnen worden gemaakt van een dataketen om volgens internationale standaarden data te kunnen sturen en ontvangen. De iVRI wordt hierin via beveiligde verbindingen verbonden aan het internet. iVRI's communiceren voortdurend met naderende voertuigen via een van de op UDAP aangesloten cloud providers. De aldus verkregen geminimaliseerde gegevens maken het op kruispuntniveau mogelijk om de verkeerslichtenregelingen efficiënter te laten verlopen. Op traject- en netwerkniveau wordt het mogelijk om verkeersstromen met dynamische regelingen van verkeerslichten efficiënter op elkaar af te stemmen. Hierdoor kan een wegbeheerder de verkeersstromen beter optimaliseren naar verschillende beleidsdoelen, zoals veiligheid, leefbaarheid, duurzaamheid en doorstroming. En krijgt de weggebruiker die van een dergelijk dienst gebruik wenst te maken meer comfort, minder onnodig wachten, een lager brandstofverbruik en meer veiligheid. Daarbij hebben weggebruikers keuze uit meerdere aanbieders en uiteenlopende diensten, gratis danwel slechts tegen betaling beschikbaar. Er is sprake van een volwassen markt met ruime diversiteit in aanbieders en diensten met uiteenlopende functionaliteiten. Deze diensten kunnen worden aangeboden op navigatieapparatuur (los of als onderdeel van het voertuig), logistieke apparatuur voor ritplanning of op smartphones (voor bijv. particulieren met een oudere generatie voertuigen en fietsers).

2.1.1 Functionaliteiten van de iVRI - Use Cases

Een VRI is een iVRI als deze verbonden is met UDAP en er zo gegevens tussen de iVRI en weggebruikers worden uitgewisseld. Naast het sturen en ontvangen van data levert een iVRI een drietal landelijk geharmoniseerde toepassingen ("Use Cases"): Prioriteren, Informeren en Optimaliseren. De drie groepen iVRI Use Cases worden hier onder nader toegelicht.

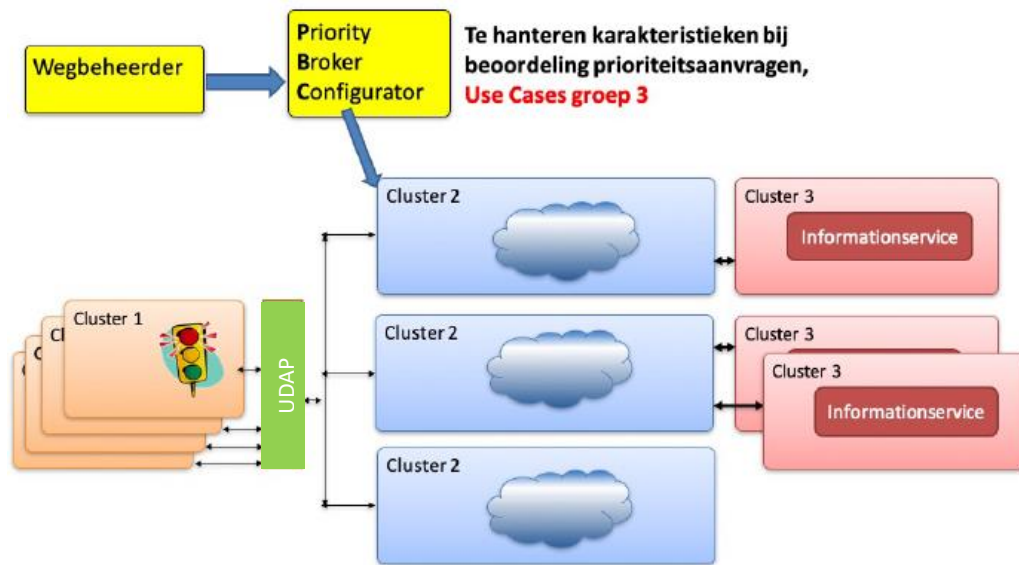
Use Case 3 - Prioriteren

Deze Use Case betreft het prioriteren van specifieke doelgroepen bij verkeerslichten, zoals hulpdiensten, lijnbussen, groepen auto's en (groepen) vrachtauto's. Dit kan ook op specifieke rijstroken. Denk aan busbanen of goederencorridors richting bedrijfsterreinen.

De keuzeruimte voor het wel of niet prioriteren (en zo ja, in welke mate) van verkeersdeelnemers wordt met de iVRI ook uitgebreid. Hoe flexibeler prioriteringssystemen zijn, hoe meer ordening en structuur nodig is om de prioriteiten goed te configureren. Om dit te faciliteren is de Priority Broker Configurator (PBC) ontwikkeld en in gebruik genomen. Met dit webbased instrument kunnen wegbeheerders zelf voor iedere individuele iVRI de criteria configureren om te komen tot een prioriteitsclassificatie van naderende voertuigen, en zo hun beleidskeuzen ten aanzien van prioriteitsverlening per doelgroep per iVRI's vastleggen en flexibel aanpassen. De PBC kan daarmee worden gezien als een moderne, meer geavanceerde versie van het KAR Geo Tool, dat DOVA (Decentrale OV-Autoriteiten) onder verantwoordelijkheid van overheden heeft ontwikkeld en beheert en waarin wegbeheerders zelf invullen welke prioriteiten zij hanteren voor openbaar vervoer op kruispunten met reguliere VRI's.

In Figuur 3 is de werking van de PBC verder toegelicht: iedere wegbeheerder vult voor elk van diens iVRI's de PBC conform de lokale beleidsuitgangspunten. Ze geven aan welk type voertuig (bijvoorbeeld 'lijnbus') welke numerieke prioriteitsniveau moeten hebben (bijvoorbeeld '5'). Partijen in Cluster 2 ontvangen locatiemeldingen vanuit de op hun service aangesloten voertuigen en toetsten aan de hand van de specifieke voertuigkenmerken in de PBC of en in welke mate het voertuig gerechtigd is om bij de eerstvolgende iVRI op de route prioriteit te krijgen. Indien dat zo is, stuurt die Cluster 2 partij via UDAP naar desbetreffende iVRI een SRM-bericht (Service Request Message), een prioriteitsverzoek inclusief het in de PBC vastgestelde numerieke prioriteitsniveau en de verwachte aankomsttijd van het voertuig bij die iVRI. Op basis van die gegevens wordt de regeling van de iVRI prioriteit zodanig aangepast, dat tijdig prioriteit kan worden verleend aan het voertuig, mits en voor zover de verkeerssituatie dit toelaat.

Na ontvangst van een SRM-bericht met een prioriteitsaanvraag, antwoordt de iVRI met een SSM-bericht (Service Support Message), dat via UDAP door de partij in Cluster 2 naar het naderende voertuig kan worden gezonden om de berijder ervan te laten weten dat de prioriteitsaanvraag is ontvangen door de iVRI. Naarmate het voertuig dichterbij de kruising komt, worden updates van eerder verzonden SRM- en SSM-berichten uitgewisseld: door de opeenvolgende aanduidingen "requested", "processing", "rejected", "granted" en "watch other traffic" in de SSM-berichten, kan door de iVRI worden gecommuniceerd of de aangevraagde prioriteit daadwerkelijk aan het voertuig zal worden verleend.



Figuur 3 Illustratie van de datastromen binnen het Partnerschap Talking Traffic

Use Case 4 - Informeren

Deze Use Case betreft het in-car verstrekken van actuele informatie vanuit de iVRI's. Het gaat daarbij om de volgende informatie:

- Huidige status (groen, geel, rood) van de iVRI die door het voertuig wordt genaderd. Daardoor kan de berijder ondanks fel tegenlicht van de zon of een zicht blokkerende vrachtwagen toch tijdig zien of kan worden doorgereden of moet worden gestopt.
- Tijd tot Rood (TTR), welke de weggebruiker in staat stelt te beoordelen of nog veilig door groen kan worden gereden, of toch maar beter snelheid kan worden verminderd om tijdig tot stilstand te komen voor het rode licht.
- Tijd tot groen (TTG), welke de weggebruiker in staat stelt beter te anticiperen op het groen worden van het verkeerslicht. Dit zorgt voor minder verliestijd bij het wegrijden bij een verkeerslicht. Op termijn zou deze informatie kunnen worden gekoppeld aan het start-stop systeem in het voertuig.
- Green Light Optimum Speed Advise (GLOSA), een op maat gesneden adviessnelheid aan de weggebruiker om voor zichzelf een groene golf te kunnen creëren.
- De reden waarom de weggebruiker (extra) moet wachten op groen licht, bijvoorbeeld door een prioriteitsingreep ten behoeve van een OV-bus of een met spoed naderend nood- en hulpdienstvoertuig. Veel verkeersdeelnemers waarderen het als ze informatie krijgen over de reden voor (extra) wachttijd.

Als gevolg van de nog altijd grote dynamiek van de regeling van de verkeerslichten in Nederland, is op verzoek van de gemeenschappelijke wegbeheerders de informatie over TTR, TTG en GLOSA momenteel nog niet ingeschakeld.

Use Case 5 - Optimaliseren

Deze Use Case betreft het optimaliseren van de verkeersafwikkeling op een of meerdere kruispunten door het beschikbaar stellen van geanonimiseerde verplaatsingsdata van weggebruikers aan de verkeersregelingen. Elke weggebruiker die een app gebruikt, kan een bron van informatie zijn voor de verkeerslichten. Uiteraard slechts indien en voor zover de weggebruiker zelf bij activering van zijn/haar informatiedienst toestemming heeft gegeven voor dergelijk datagebruik in relatie tot die geboden functionaliteit. Deze verplaatsingsinformatie is nuttig voor optimalisering van de regeling van iVRI's: hoe meer voertuigen op grotere afstand die informatie verstrekken, hoe beter de verkeerslichtenregeling hiermee rekening kan houden. Dit draagt bij aan een optimalisatie van de doorstroming en verbetering van de (fysieke) netwerkprestaties en daarmee de kwaliteit van de stad. Daarnaast is deze Use Case een prikkel voor de bouwers van een iVRI ITS-App om verdere doorstromingsverbetering te vinden.

Aanbieders van zo'n iVRI ITS-App die het verkeerslicht doet regelen, kunnen ervoor kiezen om een deel van dit rekenwerk buiten de automaat (d.w.z. buiten de hardware op het kruispunt) te laten verrichten of zelfs (bijna) het hele programma buiten de automaat te draaien. De regeling draait dan 'in de cloud' op een server met veel rekenkracht. Beide vormen zijn momenteel in gebruik: de keuze en argumentatie verschilt per wegbeheerder en per leverancier. Inmiddels is wel de overtuiging groeiend, dat ongeacht de keuze voor een verkeersregeling lokaal of in de cloud, alle apparatuur en software op afstand/remote benaderbaar moet zijn voor beheer, onderhoud, nieuwe updates en aanpassingen. Kosten spelen hierin een belangrijke rol: vanaf één locatie op afstand alle aanpassingen in één keer uitvoeren kost aanzienlijk minder dan ieder kruispunt afzonderlijk fysiek bezoeken voor het uitvoeren van een analyse of het doorvoeren van een aanpassing.

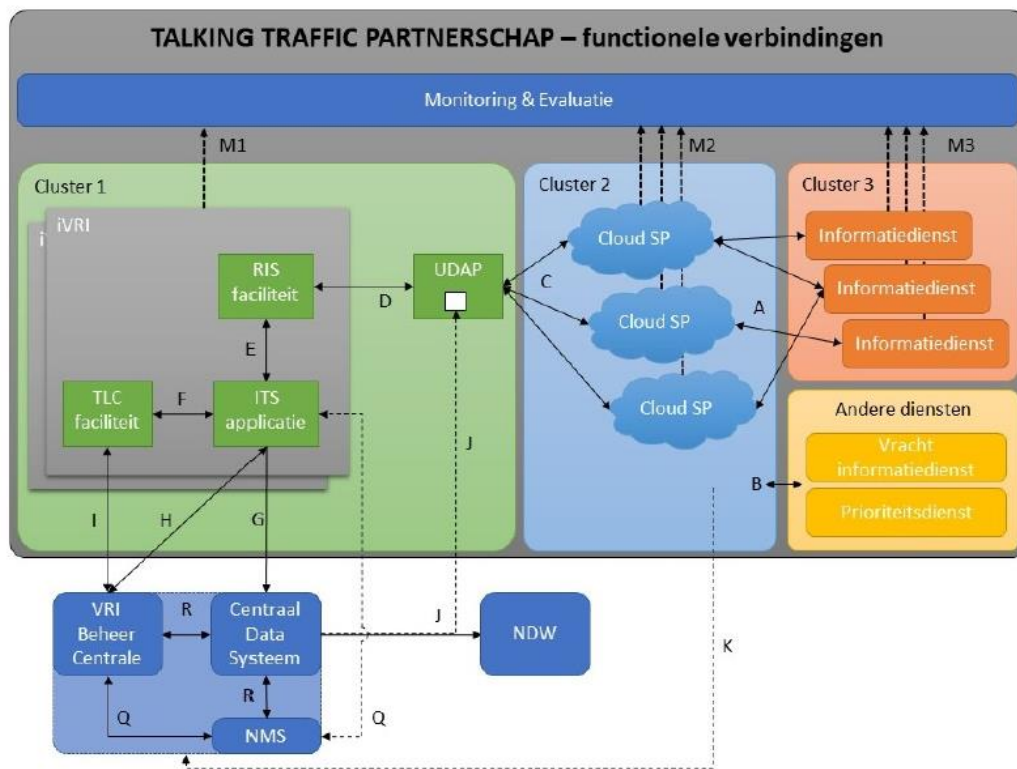
2.1.2 De iVRI standaarden

Om de Use Cases te realiseren, hebben de betrokken partijen gezamenlijk een serie standaarden ontwikkeld waarmee de verschillende onderdelen van de keten, onafhankelijk van de leverancier, met elkaar gegevens kunnen uitwisselen. De standaarden zijn gebaseerd op bestaande standaarden en zijn gelaagd opgebouwd:

- De basis bestaat uit algemene, internationale, internetstandaarden. Dit zijn door de Internet Engineering Taskforce (IETF) beheerde en gepubliceerde standaarden als TCP/IP, HTTP en TLS.
- Daarbovenop zijn er een serie Europese standaarden voor connected traffic. Deze standaarden worden door de European Telecommunications Standards Institute (ETSI) beheerd en gepubliceerd.
- De ETSI standaarden worden aangevuld en verder ingevuld met een aantal standaarden die nodig zijn om specifiek de Use Cases van Talking Traffic uit te kunnen voeren. Dit zijn de 'iVRI-standaarden', deze standaarden worden opgesteld door de bij Talking Traffic betrokken partijen en worden beheerd en gepubliceerd door CROW. In deze standaarden staat onder andere UDAP beschreven.
- Bovenop de iVRI-standaarden, zijn er de 'Dutch Profiles', deze standaarden vullen verder in hoe de verschillende datavelden uit de iVRI standaarden gebruikt moeten worden bij Talking Traffic.

2.1.3 Technische architectuur met internationaal gestandaardiseerde koppelvlakken

In Figuur 4 is de technische architectuur binnen het Innovatiepartnerschap Talking Traffic geïllustreerd. Kern is dat alle functies eenduidig zijn gespecificeerd en dat alle uitwisseling van data plaatsvindt volgens gestandaardiseerde koppelvlakken en volgens contractueel vastgelegde vereisten, die tijdens de uitvoering en gebruik ook gecontroleerd worden. De koppelvlakken voor het uitwisselen van data met de iVRI zijn allemaal internationale standaarden. Voor Nederland zijn *binnen* deze internationale standaarden verdere afspraken gemaakt en landelijk gestandaardiseerd in de zogenaamde *Dutch profiles*. Deze *Dutch profiles* voldoen dus nadrukkelijk aan de internationale afspraken en (ETSI) standaarden. Alle iVRI producten hebben een groot aantal testen moeten doorlopen om aan te tonen dat deze voldoen aan alle relevante standaarden.



Figuur 4 Illustratie van de technische architectuur binnen het Innovatiepartnerschap Talking Traffic, met (internationaal) gestandaardiseerde koppelvlakken voor het uitwisselen van data.

Het groene vlak en de beide blauwe blokken onder het grijze kader (centrales, NetwerkManagementSystemen en Nationaal Datahuis Wegverkeer) behoren tot het publieke domein; de blauwe, oranje en gele vlakken binnen het grijze kader behoren tot het private domein. De uitwisseling van verkeerslichten data vindt plaats op het scheidsvlak van groen (Cluster 1) en licht blauw (Cluster 2). In het groene vlak van Cluster 1 gaat het om tientallen wegbeheerders met elk hun eigen iVRI-leveranciers (vaak meerdere per wegbeheerder). UDAP

is in beheer van het ministerie van I&W, die de uitvoering daarvan in opdracht heeft gegeven aan Monotch.

Een iVRI bestaat altijd uit de volgende drie iVRI-functies, welke als afzonderlijke producten herkenbaar zijn:

iVRI - ITS-applicatie

De ITS-applicatie bepaalt de groensturing. Een belangrijke verandering van de ITS-applicatie in een iVRI ten opzichte van die in een conventionele VRI is dat in de iVRI de verkeersregelapplicatie (ITS-applicatie) is losgekoppeld van de hardware aansturing (TLC-faciliteit). De ITS-applicatie communiceert met de TLC-faciliteit via het gestandaardiseerde TLC-FI koppelvlak. Hierdoor kan de ITS-applicatie in principe overal draaien en van een andere leverancier zijn dan de verkeersregelautomaat. De plaatsingsmogelijkheden zijn:

- in een fysieke box in de verkeersregelautomaat;
- op het processorbord van de TLC-faciliteit;
- centraal op een server van leverancier of wegbeheerders;
- in de cloud van een leverancier.

iVRI - Roadside ITS Station (RIS)

Om een volledig coöperatieve iVRI te creëren, die in twee richtingen kan communiceren met diens omgeving, moet er een RIS-functie aanwezig zijn. Deze RIS zorgt er onder andere voor dat:

- de locatie en richting van voertuigen, fietsers en voetgangers ‘gepositioneerd’ wordt op een rijstrook. De rijstrook en de afstand tot de stopstreep worden doorgegeven aan de ITS-applicatie;
- berichten ten behoeve van Use Case “Informer” naar de voertuigen, fietsers en voetgangers worden verstuurd.

Tussen zowel de ITS-applicatie en de RIS als tussen de RIS en UDAP kunnen de volgende typen berichten worden uitgewisseld: CAM (posities van voertuigen), SRM (prioriteitsverzoeken), SSM (bevestigingen van prioriteitsverzoeken), SPAT (status van de verkeerslichten), DENM (omstandigheden op het kruispunt), IVI (berichten voor weggebruikers) en TLCCConf (component en versie informatie van de verschillende componenten van de iVRI).

De RIS is ook verantwoordelijk voor het verzenden van het MAP-bestand van de iVRI naar de weggebruikers, met daarin de configuratie van stroken en strepen op het kruispunt. Een MAP-bestand is afgeleid uit het ITF-bestand (*Intersection Topology Format*) waarin de topologie (vormgeving van het kruispunt, stopstrepen, detectie, signaalgroepen, enzovoort) is opgenomen. Op basis van deze topologie kunnen apps de gegevens van de iVRI goed interpreteren en zo de gebruiker van informatie voorzien.

De RIS kan lokaal in de verkeersregelautomaat aanwezig zijn (een kleine fysieke box), worden gehost of als software in de cloud draaien.

iVRI - TLC-faciliteit

De TLC-faciliteit is de aansturing van de hardware in de verkeersregelautomaat. Dit is eigenlijk de procesbesturing die een aantal wijzigingen heeft ondergaan om goed in de nieuwe iVRI-architectuur opgenomen te kunnen worden. Veel zaken zijn echter gebleven zoals ze waren, bijvoorbeeld het aansturen van de lichten, het uitlezen van detectielussen en andere input. Ook

de communicatie met een VRI-beheercentrale waarmee een wegbeheerder de iVRI kan beheren (verbinding I in Figuur 4) is gebleven.

De TLC-faciliteit controleert of de status van de lichten (groen, geel, rood) die aan de RIS wordt doorgegeven ook wel echt op straat wordt gerealiseerd en kan worden gerealiseerd. In theorie kan de ITS-applicatie een groensturing wensen die vanwege conflicterend groen of lopende ontruimingstijden niet is te realiseren. De TLC-faciliteit stuurt in dat geval niet het groene licht aan. Via deze link voorkomt de TLC-faciliteit ook dat de RIS informatie naar de apps verzendt die onjuist is. De TLC faciliteit heeft daarmee dus een belangrijke veiligheidsfunctie.

UDAP

Een andere belangrijke component om een iVRI in de keten te laten functioneren, is het landelijke uitwisselpunt voor iVRI-data (Urban Data Acces Platform, UDAP). Dit is het centraal overnamepunt dat als dienst, dat wil zeggen in private uitvoering onder publieke opdracht en controle van het ministerie van Infrastructuur en Waterstaat, wordt geleverd voor de geautomatiseerde uitwisseling van real-time data tussen iVRI's en weggebruikers. De gegevens van alle iVRI's worden via UDAP ontsloten. Daarmee wordt landelijke dekking gerealiseerd en is een goede bescherming en controle mogelijk op de wijze van databehandeling en -bescherming. Dankzij UDAP kan de wegbeheerder volstaan alleen met UDAP een veilige verbinding te realiseren, in plaats van met elke individuele partij in Cluster 2 (zie Figuur 2 voor een toelichting op de Clusters). Beheer, kwaliteit en databescherming zijn ook gebaat bij één landelijk uitwisselingspunt voor iVRI-data. Er is bewust voor gekozen om deze dienst door een niet-iVRI leverende private partij te laten verzorgen, zodat daarmee de onafhankelijkheid beter kan worden geborgd.

WiFi-P

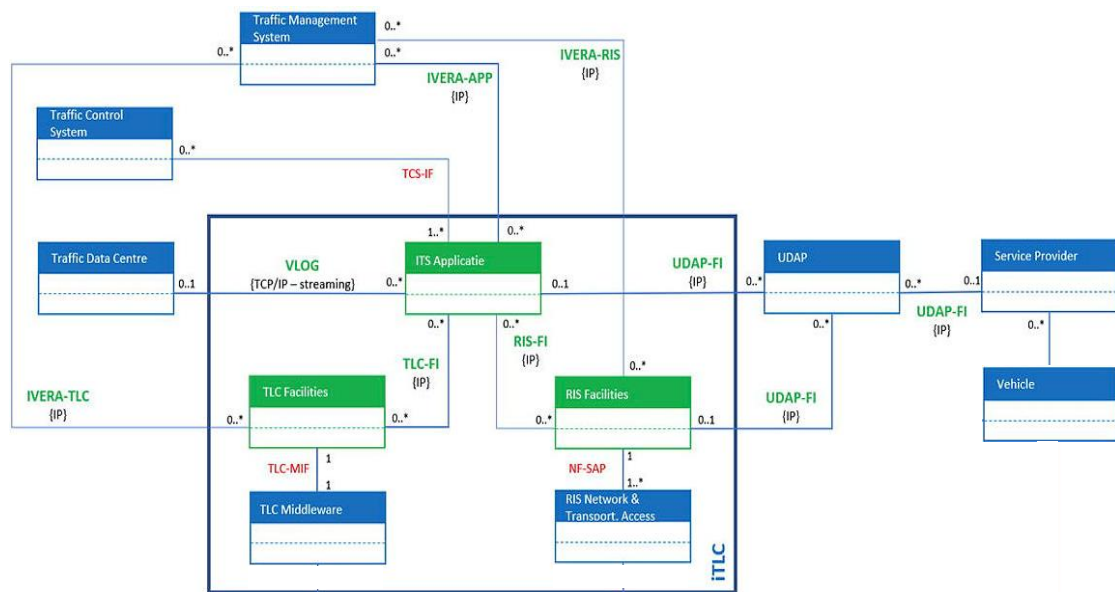
De ETSI standaarden zijn hybride, dat wil zeggen dat deze geschikt zijn voor zowel generieke TCP/IP communicatie (doorgaans via mobiele 4G/5G netwerken) als IEEE 802.11p communicatie (een variant van WiFi speciaal voor ad-hoc communicatie tussen auto's onderling en auto's en infrastructuur bij de weg). Binnen iVRI standaarden is de keuze gemaakt, conform het landelijke beleid van het ministerie van Infrastructuur en Waterstaat, om alleen generieke TCP/IP connectiviteit te gebruiken. Dit houdt in dat voorzieningen zoals privacy, security en communicatie met voertuigen en gebruikers (bijvoorbeeld fietsers) alleen worden uitgevoerd en gefaciliteerd voor communicatie via generieke netwerken. Als wegbeheerders IEEE 802.11p communicatie willen toepassen, moeten zij zelf zorgdragen voor dergelijke voorzieningen; de architectuur van de iVRI's en Talking Traffic dataketen sluiten dit niet uit. Voor de bescherming van gegevens en privacy zijn dan aangepaste maatregelen (technisch en organisatorisch) nodig.

VRI-beheercentrale

Onderdeel van de iVRI standaarden, is het IVERA-protocol. Via dat protocol kunnen de VRI-beheercentrales van publieke organisaties de verschillende componenten van de iVRI's op afstand beheren. Het IVERA-protocol heeft specifieke varianten, speciaal voor het aansturen van de TLC's, de RISsen en de ITS-applicaties.

Protocollen en interfaces

De onderstaande afbeelding geeft een overzicht van de verschillende verbindingen en de bijbehorende protocollen:



Figuur 5 Verbindingen van een iVRI

De groene blokjes geven de onderdelen van een iVRI weer. De twee blauwe blokken onder de groene blokken binnen het blauwe kader zijn componenten die horen bij een klassieke VRI (Verkeer Regel installatie). De dunne blauwe lijntjes geven communicatiestromen weer. Als de naam van een communicatie stroom in het groen is weergegeven, dan maken ze deel uit van de iVRI standaarden. De blokken binnen het blauwe kader behoren tot Cluster 1. Het blok "Service Provider", rechts van het blok "UDAP", behoort tot Cluster 2 en het blauwe blok "Vehicle", beneden het blauwe kader, zou geacht kunnen worden de voertuigapparatuur binnen Cluster 3 te representeren.

De verbindingen waarvan de iVRI standaarden eindigen met '-FI' (bijvoorbeeld 'RIS-FI') bevatten de gestandaardiseerde berichttypen (zie verderop). Deze kunnen persoonsgegevens bevatten, echter zijn deze gegevens inclusief de StationID vanwege de maximale 'time-to-life' van 5 minuten slechts kort beschikbaar. De verbindingen waarvan de naam begint met 'IVERA-' (bijvoorbeeld 'IVERA-APP') bevatten configuratie instellingen voor de verschillende onderdelen van de iVRI. Deze instellingen bevatten geen persoonsgegevens.

De TLC-FI kent ook een faciliteit om een voertuig van het ene kruispunt aan een volgend kruispunt 'over te dragen'. Deze functionaliteit maakt het in principe ook mogelijk om een voertuig over meerdere kruispunten te volgen. De VLOG stroom bevat logberichten van de iVRI. Deze logberichten bevatten mogelijk persoonsgegevens: de standaard logberichten bevatten geen persoonsgegevens, maar de leverancier van de ITS applicatie kan eigen typen logberichten toevoegen.

Gestandaardiseerde berichten

ETSI heeft een aantal gestandaardiseerde berichten gedefinieerd. Deze berichten zijn verder uitgewerkt in de iVRI-standaarden. De Dutch Profiles vullen verder in welke velden wel of niet

gebruikt mogen worden van deze gestandaardiseerde berichten en lichten het gebruik van die velden verder toe. Elk van deze berichttypen heeft een specifiek doel. De berichten worden door de keten heen gebruikt (zie ook Figuur 5):

- **CAM:** Cooperative Awareness Message. Berichten vanuit de voertuigen van weggebruikers, waarin ondermeer de actuele locatiegegevens, snelheid en rijrichting (0-360 graden) zijn opgenomen.
- **SPaT:** Signal Phase and Timing-berichten vanuit iVRI's, met ondermeer de actuele status van de signaalgroepen en de verwachte tijd tot groen of de tijd tot rood van de signaalgroepen.
- **MAP:** Dit zijn de berichten vanuit iVRI's waarin de fysieke configuratie van desbetreffend kruispunt is opgenomen.
- **SRM:** Signal Request Messages. Dit zijn de berichten vanuit voertuigen van weggebruikers (door hun cloud provider via UDAP verzonden) naar wegkantssystemen (iVRI's) ten behoeve van de prioriteitsaanvraag. De Dutch Profiles bepalen dat velden ten behoeve van de locatievermelding in deze berichten niet gebruikt worden, maar dat een SRM bericht altijd gekoppeld moet zijn aan een CAM bericht. Met betrekking tot die prioriteitsaanvragen gaat het vooralsnog met name om openbaar vervoer, nood- en hulpdiensten en vrachtverkeer. De cloud provider is verantwoordelijk voor het omzetten van het voertuigtype naar het correctie prioriteitsniveau voor die specifieke iVRI.
- **SSM:** Signal Status Message. Dit zijn de berichten vanuit wegkantssystemen (iVRI's) (via UDAP, een cloud provider en een service provider) naar een weggebruiker, waarin de iVRI communiceert of de aangevraagde prioriteit al dan niet is toegekend.
- **DENM:** Dit type berichten bevatten gegevens over gevaarlijke of abnormale/afwijkende situaties op de weg. Deze berichten worden vooralsnog nauwelijks gebruikt binnen de Talking Traffic dataketen en de UDAP geeft ze niet door. Wel is het plan om op korte termijn DENM berichten over naderende prioriteitsvoertuigen door te geven (Emergency Vehicle Approaching).

Tijdelijke Identifiers: om te voorkomen dat natuurlijke personen of hun vervoermiddelen, dan wel de vervoermiddelen waarin of waarop zij zich bevinden buiten het doelbereik van een iVRI kunnen worden gevolgd, herkenbaar zijn of getraceerd kunnen worden, worden de CAM berichten (zie hierboven) niet gekoppeld aan een persoon of een voertuig maar aan een zeer tijdelijke identiteit. Telkens wanneer een persoon of een voertuig een andere iVRI nadert, zou de desbetreffende cloud provider een nieuwe tijdelijke Identifier aan moeten maken voor deze weggebruiker en die nieuwe Identifier opnemen in de CAM berichten die gedurende diens naderingstraject naar die iVRI worden gezonden. Voor iedere nadering van een iVRI op de route van een weggebruiker wordt aldus een andere Identifier gebruikt. Opeenvolgende tijdelijke Identifiers zouden niet gerelateerd of aan elkaar te relateren moeten zijn en zouden nergens moeten worden nergens bewaard of opgeslagen. Een iVRI, iVRI- leverancier en wegbeheerder aan de 'linkerkant' van UDAP zou daardoor alleen 'losse' CAM berichten moeten zien die alleen aangeven dát er een voertuig de iVRI nadert. Door alleen zeer tijdelijke Identifiers (StationID's; zie hieronder bij 3.1.1.) te gebruiken, zouden de CAM berichten niet te herleiden moeten zijn tot een persoon of voertuig en ook niet aan elkaar te koppelen, bijvoorbeeld om hieruit een herkomst, bestemming, route of natuurlijke persoon af te leiden. Uit de technische analyse van de Cluster 2/3 partijen (zie bijlage 2) blijkt dit mechanisme niet door allen volledig juist te worden gehanteerd. Het gaat dan om herleidbare of voorspelbare StationID's, routes die niet als CAM berichten met losse punten doorgegeven worden maar

als langere segmenten en het bewaren, opslaan en doorgeven van de route historie over een langer traject dan van een kruising. Hierdoor kan het voor de wegbeheerder mogelijk worden om een voertuig over langere afstanden te volgen. Zie verder hoofdstuk 3.

Samengevat betekent dit:

- De SPaT en MAP berichten worden gegenereerd door de iVRI en worden via UDAP, cloud providers en service providers doorgeven aan hun weggebruikers (Use Case Informeren);
- De CAM berichten worden gegenereerd door voertuigen van weggebruikers om zich 'zichtbaar' te maken voor iVRI's op hun route (Use Case Optimaliseren);
- De SRM berichten worden gegenereerd door cloud providers ten behoeve van prioriteitsaanvragen voor bij hun aangesloten voertuigen (overwegend professionele doelgroepen) (Use Case Prioriteren);
- Ter bevestiging op de goede ontvangst van een SRM bericht stuurt een iVRI middels UDAP, cloud providers en service providers een SSM bericht terug aan desbetreffende weggebruiker (Use Case Prioriteren);
- De DENM berichten kunnen door verschillende partijen, waaronder iVRI's, gegenereerd worden, maar binnen de Talking Traffic dataketen worden deze vooralsnog nauwelijks gebruikt en niet door UDAP doorgegeven.

2.2 MEER WETEN?

Voor een uitgebreidere toelichting op de Use Cases, de werking van een iVRI en de stappen die nodig zijn om een iVRI te operationaliseren wordt verwezen naar het Stappenplan iVRI (zie <https://www.crow.nl/thema-s/verkeersmanagement/landelijke-ivri-standaarden> of de directe [download](#)).



3 DE IVRI EN PRIVACY

3.1 DATA VAN EN NAAR IVRI'S IN RELATIE TOT PRIVACY

Binnen de dataketen van Talking Traffic stuurt en ontvangt een iVRI meerdere typen data. Vanuit privacy is het belangrijk is om o.a. te bepalen welke van deze typen data daadwerkelijk persoonsgegevens bevatten en daarmee onder het regime van de AVG vallen. En tot waar de verantwoordelijkheid strekt en eindigt van de individuele wegbeheerder/overheid, diens iVRI-leverancier (Cluster 1) resp. waar private partijen in de Clusters 2 en 3 hun verantwoordelijkheid, maatregelen en begrenzings kennen en uitvoeren.

3.1.1 Data van en naar iVRI's

Persoonsgegevens

Onder de AVG wordt een persoonsgegeven gedefinieerd als informatie over een geïdentificeerde of identificeerbaar natuurlijk persoon.³ Het gaat om informatie over een persoon van wie de identiteit duidelijk is of aan de hand van aanvullende informatie kan worden vastgesteld. Dus, elk soort informatie kan een persoonsgegeven zijn, mits het betrekking heeft op een geïdentificeerde of identificeerbaar persoon.

Direct of indirect identificeerbaar

Om vast te stellen of een persoon identificeerbaar is, moet rekening worden gehouden met alle redelijke middelen die kunnen worden gebruikt om de persoon direct of indirect te identificeren.⁴ Identificatie vereist dus elementen die een persoon zodanig beschrijven dat hij of zij kan worden onderscheiden van alle andere personen en als individu kan worden herkend. De naam van een persoon is een voorbeeld van dergelijke beschrijvings-elementen, en kan een persoon direct identificeren.

Bij indirect geïdentificeerde of identificeerbare personen gaat het doorgaans om een aantal 'unieke combinaties'. In gevallen waarin het op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen één bepaalde persoon te onderscheiden, kan die persoon wellicht toch identificeerbaar zijn doordat aan de hand van die informatie in combinatie met andere gegevens (die al dan niet bij de verwerkingsverantwoordelijke rusten) de betrokkene van andere personen kan worden onderscheiden.⁵

Gepseudonimiseerde persoonsgegevens

Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over identificeerbare natuurlijke persoon worden beschouwd.⁶ Persoonsgegevens bevatten attributen, zoals naam, geboortedatum, geslacht, adres, of andere elementen die tot identificatie kunnen leiden. Het proces van het pseudonimiseren van persoonsgegevens houdt in dat deze attributen worden vervangen door een pseudoniem. Persoonsgegevens kunnen dan niet langer aan een specifieke betrokkene worden toegeschreven zonder dat gebruik wordt gemaakt van aanvullende informatie, mits deze aanvullende informatie afzonderlijk wordt bewaard en er waarborgen zijn geïmplementeerd dat de persoonsgegevens niet aan een natuurlijke persoon worden

³ Artikel 4 lid 1 AVG.

⁴ Overweging 26 AVG.

⁵ Groep Gegevensbescherming artikel 29, Advies 4/2007 over het begrip persoonsgegevens, p. 14-15.

⁶ Overweging 26 AVG.

toegeschreven.⁷ In tegenstelling tot anonieme gegevens, zijn gepseudonimiseerde gegevens nog steeds persoonsgegevens en vallen zij dus onder de AVG.

Persoonsgegevens in een dataketen

Als gegevens in een dataketen tussen partijen worden uitgewisseld, moet er rekening mee worden gehouden dat er zowel sprake kan zijn van direct als indirect herleidbare persoonsgegevens die iedere partij afzonderlijk verstrekt of verder verwerkt. Er moet daarbij altijd worden beoordeeld of op worden gelet of de partijen in de keten gezamenlijk dan wel individueel in staat zijn om de ontvangen gegevens te herleiden tot een individu. Daarbij moet niet alleen rekening worden gehouden met de gegevens zoals deze tussen partijen uitgewisseld worden in de keten. Het is belangrijk dat ook rekening wordt gehouden met de ‘overige’ gegevens waar een partij individueel over beschikt.

Waar een bepaald gegeven, zoals bijvoorbeeld locatie, voor één van de partijen in de dataketen niet herleidbaar is tot een individu, kan dit voor andere partijen wel herleidbaar zijn. Dit vanwege hun rol in de keten of juist doordat zij beschikken of geautoriseerd toegang hebben tot andere databanken, zodat zij door de toegang tot meer informatie ook gegevens kunnen combineren en zodoende verbanden *kunnen* leggen, waardoor informatie wel herleidbaar kan zijn tot personen. Immers, voor het indirect identificeren van een persoon heeft een partij doorgaans een combinatie van gegevens nodig. Doordat een iVRI een Pseudo-ID van het OV-voertuig respectievelijk de eindgebruiker van een app ontvangt, zou het voor de meeste wegbeheerders niet mogelijk moeten zijn om de bestuurder direct dan wel indirect te identificeren. Maar, als een wegbeheerder voor haar eigen wagenpark bijvoorbeeld gebruik wil gaan maken van een service provider uit Cluster 3 zou er een andere situatie kunnen ontstaan. Door als wegbeheerder een bepaalde prioritering toe te kennen aan voertuigen van specifieke medewerkers, zoals bijvoorbeeld wegingspecteurs, kan aan de hand van de gegevens over het voertuig die naar de iVRI worden verzonden, in combinatie met gegevens uit het eigen personeelsbestand en wagenpark, door die wegbeheerder mogelijk achterhaald worden welke wegingspecteur het was die op een bepaald moment een bepaalde iVRI passeerde. Zonder afdoende waarborgen te treffen zal hierdoor de situatie kunnen ontstaan dat er mogelijk sprake is van een onrechtmatig personeelsvolgsysteem, dan wel dat de data wordt gebruikt voor andere, mogelijk niet-verenigbare doeleinden.

Daarnaast zou ook sprake kunnen zijn van herleidbaarheid tot een persoon, doordat de informatie kan worden gecombineerd met andere beschikbare bronnen. Dit kan bijvoorbeeld ook in het geval de partij diverse rollen vertegenwoordigt in de dataketen. Indien gegevens in de keten tussen partijen worden uitgewisseld én een van de partijen de uitgewisselde gegevens kan herleiden (direct of indirect) tot een individu, is er sprake van het verwerken van een persoonsgegeven of -gegevens in de dataketen.

Data die een iVRI uitstuurt, maar niet worden gebruikt binnen de Talking Traffic dataketen

Een iVRI stuurt V-Log data uit, wegbeheerders gebruiken deze data voor het beheren van hun iVRI's. V-Log is een soort logboek (in de iVRI) die het functioneren van de iVRI bijhoudt. De V-Log kan gegevens van de iVRI zelf bevatten, maar ook gegevens van externe bronnen. Dat kunnen gegevens uit de iVRI dataketen zijn, maar dat kunnen ook gegevens van andere bronnen zijn, zoals van de detectielussen en KAR, VETAG en VECOM signalen. Op zo'n manier komen er in de logs ook gegevens zoals wanneer een detectielus bezet is en hoe lang, of het ID-nummer van een bus als deze prioriteit aanvraagt via VECOM. Het is mogelijk om de

⁷ Artikel 4 lid 5 AVG.

detectorgegevens uit V-Log berichten te combineren met andere databronnen, zoals videocamera's bij kruispunten, waardoor deze combinatie mogelijk is te herleiden tot een natuurlijk persoon. Daarmee zijn V-Log data ook privacygevoelig. V-Log data worden echter niet gebruikt in de dataketen van Talking Traffic. De discussie of V-Log data wel of niet privacygevoelig zijn, is daarom geen opgave voor het programma Talking Traffic; juridisch advies dat lenW bekend is, wijst er op dat V-log datastroom gegevens bevat die mogelijk privacygevoelig kunnen zijn. Het is daarom aan de wegbeheerder om passende maatregelen aangaande de AVG te treffen. Dit geldt ook voor andere databronnen en het gebruik daarvan door wegbeheerders buiten de Talking Traffic keten, zoals conventionele VRI's en ANPR-camera's (kentekencamera's), verkeerscamera's en toepassingen daarvan voor verkeersmanagement, stadsbeheer of andere activiteiten van een waterschap, gemeente, provincie of Rijkswaterstaat.

Data die een iVRI uitstuurt

Om de toegelichte functies in de dataketen te kunnen vervullen, stuurt een iVRI de volgende typen data uit:

- SPaT berichten: de berichten vanuit de iVRI naar weggebruikers over de beeldstanden van de lampen en de verwachte tijd tot groen licht of de tijd tot rood licht;
- SSM berichten: de berichten vanuit de iVRI naar weggebruikers om aan te geven of de aangevraagde prioriteit al dan niet wordt toegekend;
- MAP berichten: berichten van de iVRI naar de weggebruikers waarin de lay-out van het kruispunt wordt doorgegeven.
- DENM berichten: berichten vanuit een iVRI met codes over blokkades op het kruispunt en mogelijke oorzaken daarvan. Deze worden vooralsnog nauwelijks gebruikt binnen de Talking Traffic dataketen.

Al deze datatypen betreffen internationale standaarden; binnen deze internationale standaarden zijn voor Nederland nadere detailafspraken gemaakt en vastgelegd in *Dutch profiles*. Een iVRI stuurt deze datatypen uit naar UDAP, die deze vervolgens verder doorstuurt in de dataketen naar de cloud providers (Cluster 2) en service providers (Cluster 3), waarna deze worden omgezet in informatie ten behoeve van de weggebruikers. De inhoud van deze datatypen betreft *state and status* van de iVRI en het kruispunt. Dat wil zeggen 'welke kleur toont het licht', 'wanneer wijzigt de kleur van het licht', 'wat is de oorzaak van een verlengde wachttijd (bijvoorbeeld in verband met prioriteitsverlening OV, naderend hulpdienstvoertuig, etc.)' en 'hoeveel rijstroken heeft het kruispunt, hoe lang zijn deze rijstroken en waar ligt de stopstreep'.

De MAP en SPaT berichten bevatten geen persoonsgegevens, ook niet als meta-data en vallen dus buiten de reikwijdte van de AVG. Voor het delen van deze berichten als Open Data, moet een aparte analyse gemaakt worden van de mogelijke veiligheidsrisico's.

De SSM berichten bevatten twee ID's (MessageID en StationID) die direct terugwijzen naar het SRM bericht en de CAM berichten waar het SSM bericht een antwoord op is. Daardoor bevat het SSM bericht persoonsgegevens.

Data die een iVRI ontvangt

Om de toegelichte functies in de dataketen te kunnen vervullen, ontvangt een iVRI de volgende typen data uit de dataketen:

- SRM berichten: Deze berichten betreffen de aanvraag vanuit voertuigen van weggebruikers (door hun cloud provider via UDAP verzonden) naar wegkantssystemen (iVRI's) ten behoeve van de aanvraag van prioriteit op het kruispunt. De cloud provider bepaalt aan de hand van de voertuigeigenschappen en de door de wegbeheerder in de PBC (Priority Broker Configurator) opgenomen criteria of het voertuig gerechtigd is tot aanvraag van prioriteit, en zo ja, in welke mate ("prioriteitsklasse"). Aan de hand

daarvan stelt deze het SRM bericht op en verzendt dit via UDAP naar de iVRI. Het betreft hierbij doorgaans doelgroepen als openbaar vervoer, nood- en hulpdiensten en vrachtverkeer. Een SRM-bericht bevat een tijdelijke unieke identifier en is altijd, via het StationID, gekoppeld aan een CAM bericht.

- CAM berichten: Berichten van weggebruikers naar de iVRI. CAM berichten bevatten onder andere het tijdelijke ID (StationID), de positie, rijrichting en snelheid van het voertuig, indien bekend de lengte van het voertuig, indien bekend in welke richting het voertuig afslaat. Verder bevat het velden voor de ervoor afgelegde route en, als het een openbaarvervoersvoertuig is, details over het voertuignummer en lijnnummer. Over deze laatste velden zegt de Dutch Profiles dat ze niet gebruikt mogen worden. Bij noodritten van hulpdiensten raadt de Dutch Profile aan om aan te geven naar wat voor een soort incident het voertuig onderweg is door een DENM bericht in het CAM bericht op te nemen. Dit type berichten worden echter niet door de UDAP doorgegeven.

Het StationID van de CAM en SRM berichten die UDAP ontvangt ter doorzending aan een iVRI zou stabiel moeten zijn gedurende het naderingstraject van een voertuig naar een iVRI. Ten behoeve van de berichtenuitwisseling met de eerstvolgende iVRI op de route van dat voertuig zou een nieuwe ID willekeurig opnieuw gegenereerd moeten worden. Daardoor zou de wegbeheerder niet in staat moeten zijn om een voertuig langs meerdere verkeersregelininstallaties te volgen. Binnen dat naderingstraject van een voertuig richting een kruising is het StationID echter stabiel. Daardoor is gedurende dat traject sprake van een indirect identificerend gegeven en zijn de CAM en SRM berichten een persoonsgegeven. De beperking van het gebruik van een ID tot dat naderingstraject van een iVRI werkt wel als privacy by design maatregel om verdergaande heridentificatie tegen te gaan. Die maatregel is afhankelijk van het correct genereren van het StationID door de cloud provider (Cluster 2). Uit de technische analyse (zie bijlage 2) bleek dat niet altijd correct te verlopen.

Daarnaast is heridentificatie door de wegbeheerder ook mogelijk aan de hand van andere gegevens binnen het CAM of SRM bericht. Bij openbaarvervoervoertuigen bevatten de standaarden een aantal velden voor andere, externe ID's, zoals het voertuig ID en lijnnummer. De Dutch Profile schrijft voor dat deze velden met een nul gevuld moeten worden. Het niet correct uitvoeren hiervan kan alsnog heridentificatie via de CAM en SRM berichten mogelijk maken.

Een aantal verschillende kenmerken van een voertuig, die los van elkaar niet indirect identificerend zijn, kunnen in combinatie wel indirect identificerend zijn. Zo'n combinatie maakt het ook mogelijk om de afgelegde route in kaart te brengen en de weggebruiker te heridentificeren. De CAM berichten bevatten geen combinatie van gegevens die op eerste gezicht indirect identificerend zijn, maar de exacte grootte van dit risico kan alleen ingeschat worden met een statistische analyse.

Voor prioriteitsgerechtigde voertuigen kan de cloud provider tot maximaal 5 minuten voor aankomst op de stopstreep van een kruising het SRM bericht naar de iVRI sturen, vergezeld van de aanduiding op welke signaalgroep de aanvraag betrekking heeft, zodat het juiste licht op het juiste (ETA) moment op groen kan worden gezet. Vervolgens wordt er iedere 10 seconden een update van de SRM verzonden, zodat de regeling van de iVRI kan worden aangepast als er sprake is van een eventuele wijziging van de eerder aangegeven ETA. Door deze berichten is het prioriteitsvoertuig voor de wegbeheerder over dat naderingstraject te volgen. De privacy impact hiervan is echter beperkt omdat uit deze gegevens noch de identiteit van de chauffeur nog die van eventuele passagiers te herleiden zijn.

Verwerkersovereenkomsten

Talking Traffic eist dat wegbeheerders met hun iVRI-leveranciers en de iVRI-leveranciers met UDAP verwerkersovereenkomsten afsluiten. Daarin wordt geborgd dat de tijdelijke StationID's

wel gebruikt worden voor de regeling van een verkeerslicht, maar niet bewaard worden na die geautomatiseerde handeling. Tevens is de afspraak gemaakt dat UDAP uitsluitend de van cloud providers (Cluster 2) ontvangen berichten levert aan de iVRI's van wegbeheerders waarvan geregistreerd is dat deze daartoe een verwerkersovereenkomst hebben afgesloten met hun iVRI-leveranciers. Naleving hiervan wordt bewaakt door IenW.

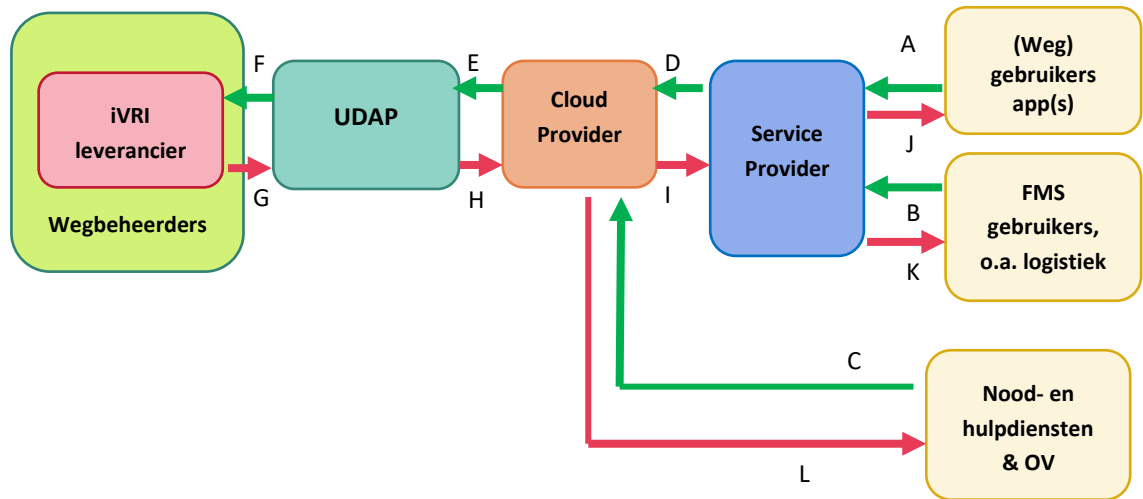
De CAM en SRM berichten zijn gepseudonimiseerde persoonsgegevens. De maatregel die genomen is om te voorkomen dat wegbeheerders deze gegevens kunnen heridentificeren, het gebruik van een unieke StationID in de berichtenuitwisseling van een voertuig met een specifieke iVRI, die slechts gedurende het naderingstraject van dat voertuig richting die specifieke iVRI stabiel is, blijkt bij enkele partijen als gevolg van onjuiste hantering in de praktijk onvoldoende waarborgen te geven tegen heridentificatie.

3.1.2 Het gebruik van iVRI-data per schakel in de dataketen

In de onderstaande figuren is geïllustreerd hoe CAM- en SRM-berichten worden gebruikt in de rest van de dataketen (de **groene en rode** pijlen geven aan in welke richting de berichten worden gestuurd):

- Reguliere weggebruikers, vooralsnog doorgaans gebruikers van een app, en berijders van prioriteitsgerechtigde voertuigen (zoals logistiek en OV-bussen) die nog gebruik maken van een app, geven aan 'hun' service provider middels het instemmen met het eigen privacy statement van de service provider, instemming om hun verplaatsingsgegevens te gebruiken voor specifieke doeleinden. Deze verplaatsingsgegevens van die weggebruikers komen terecht bij 'hun' service provider;
- Binnen deze toestemming geeft een service provider aan 'zijn' cloud provider, d.w.z. de cloud provider waarmee de service provider een zakelijk afspraak heeft, instemming voor het gebruik van verplaatsingsgegevens, wederom voor specifieke doeleinden en binnen de voorwaarden waar de eindgebruiker die bron is van deze data, mee heeft ingestemd;
- De professionele organisaties met weggebruikers, zoals de nood- en hulpdiensten, OV-vervoerders en de logistieke sector beschikken veelal over vast voertuigapparatuur en maken met hun leveranciers daarvan afspraken over de wijze waarop CAM en SRM berichten door de cloud provider(s) (Cluster 2) naar UDAP worden verzonden;
- De cloud providers doen vervolgens binnen de initiële toestemming die de weggebruiker/klant heeft verleend aan zijn service provider, hetzelfde met UDAP. Volgens deze lijn en relatie komen CAM- en SRM-berichten, met tijdelijke unieke identifiers zoals hierboven beschreven, terecht bij UDAP;
- Een wegbeheerder, maar feitelijk diens iVRI leverancier, ontvangt CAM- en SRM-berichten van UDAP. En gebruikt deze uitsluitend en alleen binnen de initiële instemming die de weggebruiker heeft verleend aan zijn service provider (en dus niet voor andere toepassingen) en als vastgelegd in de eigen verwerkersverantwoordelijkheid als wegbeheerder en verwerkersovereenkomst met diens iVRI leverancier;
- Een wegbeheerder geeft diens iVRI-leveranciers expliciete instemming om ten behoeve van het regelen van het verkeer middels iVRI's, de CAM- en SRM-berichten te gebruiken;
- Vanuit deze rol en vastlegging in een overeenkomst geven iVRI leveranciers aan UDAP hun instemming om hiertoe CAM- en SRM-berichten te ontvangen.

Het doorsturen van de CAM-, SRM en SSM-berichten in de dataketen vormt de basis voor verwerkersverantwoordelijkheden en het afsluiten van verwerkersovereenkomsten.



Figuur 6 Illustratie van het gebruik van data van en voor iVRI's in de dataketen van Talking Traffic

In de dataketen worden door partijen CAM- en SRM-berichten ten behoeve van de iVRI's verzonden op de volgende koppelvlakken/interfaces:

- A. Reguliere weggebruikers (doorgaans gebruikers van apps) en bestuurders van prioriteitsgerechtigde voertuigen (zoals vrachtwagens) die nog gebruik maken van een app: CAM
- B. Zakelijke/professionele weggebruikers middels FMS (Fleet Management Systemen): CAM;
- C. Prioriteitsgerechtigde voertuigen (Nood- en hulpdiensten, OV en logistiek): CAM;
- D. CAM;*
- E. CAM en SRM
- F. CAM en SRM

*NB: bij een service provider worden de SRM berichten in de app van de weggebruiker gegenereerd. Bij die serviceprovider worden de SRM-berichten ook verzonden over koppelvlakken A, B en C.

Binnen de dataketen worden vanuit de iVRI's richting de weggebruikers MAP, SPaT, SSM en DENM berichten verzonden. In de keten verloopt dit als volgt:

- G. wegbeheerder (iVRI leverancier, Cluster 1) naar UDAP: MAP, SPaT, SSM en mogelijk ook DENM;
- H. UDAP naar cloud provider (Cluster 2): MAP, SPaT en SSM, mogelijk ook DENM;
- I. cloud provider (Cluster 2) naar service provider (Cluster 3): MAP, SPaT en SSM, mogelijk ook DENM;
- J. service provider (Cluster 3) naar weggebruikers app: MAP, SPaT en SSM, mogelijk ook DENM;
- K. service provider (Cluster 3) naar weggebruikers FMS: MAP, SPaT en SSM, mogelijk ook DENM;

- L. cloud provider (Cluster 2) naar nood- en hulpdiensten en OV: MAP, SPaT en SSM, mogelijkserwijs ook DENM.

Een voorbeeld hiervan is een bus die prioriteit aanvraagt. Het on-board systeem van de bus communiceert met de eigen back-end. Die back-end stuurt een CAM bericht aan de gecontracteerde cloud provider. De gecontracteerde cloud provider beoordeelt aan de hand het ontvangen CAM bericht en de inhoud van de PBC (Priority Broker Configurator) of 'ie op de eerstvolgende kruising prioriteit voor de bus kan aanvragen. Als dat het geval blijkt, stuurt de cloud provider een SRM bericht via UDAP naar de iVRI. Deze zendt in antwoord een SSM bericht terug. Zodra zeker is dat de aangevraagde prioriteit daadwerkelijk door de iVRI verleend zal kunnen worden, stuurt deze (via UDAP en de cloud provider) aan de bus een SRM bericht met de status "granted". Totdat de bus de stopstreep op kruising passeert, blijft de bus met CAM en SRM berichten de iVRI op de hoogte houden van diens actuele positie en verwachte ETA.

Om het prioriteitsverzoek te kunnen beoordelen, moet de iVRI een aantal zaken weten:

- De actuele positie van de bus; het CAM bericht bevat deze gegevens.
- De verwachte aankomsttijd van de bus op de stopstreep van de kruising; het SRM bericht bevat dit gegeven.
- De prioriteitsklasse van de bus; het SRM bericht bevat dit gegeven.
- De signaalgroep waarvoor de prioriteit wordt aangevraagd; het SRM bericht bevat dit gegeven.
- Of het voertuig prioriteitsgerechtigd is en welke numerieke prioriteit het voertuig moet hebben, dit is door de cloud provider vastgesteld.

Op deze manier kan de bus, zonder extra velden die heridentificatie mogelijk maken, prioriteit aanvragen.

Figuur geeft de datastroom *in* de keten van Talking Traffic weer. Zowel wegbeheerders (Cluster 1) als Cluster 3 dienstverleners kunnen gegevens uit de Talking Traffic keten combineren met gegevens uit andere bronnen. Vanuit Cluster 1 kunnen dergelijke gegevens via DENM berichten in de keten terecht komen, dit speelt vooral als er meer typen DENM berichten toegestaan worden. Binnen Cluster 1 en binnen Cluster 3 kan door het combineren van de gegevens van Talking Traffic met andere gegevens verwerkingen ontstaan die buiten de Talking Traffic keten om verlopen. Zulke verwerkingen moeten apart beoordeeld worden en vallen buiten de scope van deze DPIA.

3.2 VERWERKINGSVERANTWOORDELIJKE EN VERWERKER

Een verwerkingsverantwoordelijke is een natuurlijk 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.⁸ De verwerker is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt, dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.⁹

⁸ Art. 4 lid 7 AVG

⁹ Art. 4 lid 8 AVG

3.2.1 Verwerkingsverantwoordelijken

Zowel de wegbeheerders als de service providers (Cluster 3) zijn beiden verwerkingsverantwoordelijke. Elk vanuit een eigen verantwoordelijkheid en grondslag. De wegbeheerder heeft de taak en verantwoordelijkheid vanuit de Wegenverkeerswet om op kruispunten het verkeer veilig en efficiënt te regelen met verkeerslichten. Deze kan er vervolgens voor kiezen om dit te doen met een iVRI en bepaalt binnen welke beleidskaders deze iVRI dient te functioneren. Doordat de wegbeheerder het doel (verkeer veilig en efficiënt regelen) en de middelen (iVRI) vaststelt, is de wegbeheerder voor het verwerken van persoonsgegevens, in het kader van de iVRI, de verwerkingsverantwoordelijke. Dit vloeit voort uit en hangt samen met diens publieke taak. Zie hierover verder de grondslag voor de verwerking in paragraaf 3.3.

De service providers (Cluster 3) hebben tot doel om hun klanten, de gebruikers van hun applicaties, te voorzien van uitgebreide reis en rijtaak ondersteunende informatie ten behoeve van onder andere meer comfort, lagere emissies en hogere veiligheid. Dit doen zij door zowel data te verzamelen van hun klanten (verplaatsingsgegevens in de vorm van CAM-berichten) middels een applicatie op bijvoorbeeld een telefoon, als door het teruggeven van bepaalde data vanuit de iVRI en cloud providers (Cluster 2) aan deze klanten. Hiermee kunnen de service providers (Cluster 3) ook gekwalificeerd worden als verwerkingsverantwoordelijke.

De cloud providers (Cluster 2) zorgen namens de service providers (Cluster 3) voor de doorgifte van de klantdata middels UDAP naar de iVRI-inrichtingen van de wegbeheerders. De cloud providers handelen hierbij als verwerker van de service provider. Wel is uit de analyse gebleken dat diverse cloud- en service providers en leveranciers van iVRI-componenten (TLC, ITS als RIS), de Cluster 1 leveranciers, als entiteiten juridisch met elkaar zijn verweven. Dit kan in de praktijk een risico vormen indien een iVRI-leverancier ook actief is als cloud provider en/of als service provider, omdat de leverancier dan buiten UDAP om een communicatiestroom tussen Cluster 1 enerzijds en Cluster 2/3 anderzijds kan opzetten, dan wel dat er toegang mogelijk is tot data die wordt verwerkt in de systemen van de Cluster 1 partij door de Cluster 2/3 partij en vice versa.

Samenvattend: zowel wegbeheerders als de partijen die optreden als service provider zijn verwerkersverantwoordelijken. Dit gelet op hun eigen publieke taken, respectievelijk aanbieders van informatiediensten met betrekking tot de CAM, SRM, SSM en DENM berichten binnen de dataketen van Talking Traffic.

UDAP onder verantwoordelijkheid van lenW

Ten opzichte van de eerste versie van de ketenbrede PIA Talking Traffic moet ons inziens UDAP (met lenW als verantwoordelijke) niet worden aangemerkt als verwerker. Om de rollen en verantwoordelijkheden binnen de Talking Traffic dataketen te beoordelen, is op grond van de AVG vooral de feitelijke situatie van belang. Zoals in hoofdstuk 2 al beschreven, is het lenW die binnen haar publieke taken het initiatief heeft genomen tot het instellen en inrichten van UDAP. Zij bepaalt hierbij hoofdzakelijk het doel en de middelen waarop de verwerking van persoonsgegevens binnen UDAP plaatsvindt. UDAP fungeert hierbij als doorgiftepunt van de data benodigd voor de iVRI-prioriteringsaanvragen. Deze data wordt vanuit de iVRI's van de wegbeheerders (middels hun iVRI-leveranciers, Cluster 1) weer doorgegeven aan uiteindelijk de weggebruikers. Feitelijk is UDAP de centrale schakel in de gegevensuitwisseling tussen weggebruikers en de iVRI's van wegbeheerders. De service providers (Cluster 3) en cloud providers (Cluster 2) hadden immers ook met de individuele wegbeheerders afspraken over de overdracht van de data kunnen maken, en dit ook technisch als zodanig in kunnen richten.

Monotch faciliteert en beheert UDAP onder verantwoordelijkheid van lenW. lenW heeft hiervoor met Monotch een verwerkersovereenkomst gesloten. Dit betekent dat gelet op de

relatie verwerkingsverantwoordelijke, verwerker en de verwerkersovereenkomst voor UDAP tussen lenW en Monotch niets verandert.

Gelet op de feitelijke situatie pleiten wij er dan ook voor dat lenW zelfstandig verantwoordelijk is voor UDAP (met Monotch als verwerker van lenW). Omdat middels UDAP er wel een gegevensoverdracht tussen de wegbeheerders en cloud providers (Cluster 2) plaatsvindt, maar deze partijen niet het doel en de middelen van UDAP – al dan niet tezamen met lenW – bepalen, is er geen sprake van een verwerkersrelatie tussen de wegbeheerders en UDAP als (sub)verwerker enerzijds en de cloud providers (Cluster 2) en UDAP als (sub)verwerker anderzijds. Verder hebben de wegbeheerders en cloud providers (Cluster 2) geen gemeenschappelijke verantwoordelijkheid ten aanzien van het functioneren van UDAP. Dit ligt louter bij lenW. Om te zorgen voor een zorgvuldige gegevensoverdracht tussen de partijen middels UDAP adviseren wij dat de wegbeheerders en de cloud providers (Cluster 2) met lenW een gegevensuitwisselingsovereenkomst sluiten.

3.2.2 Verwerkers

De iVRI-leveranciers (Cluster 1) en de cloud providers (Cluster 2) zijn verwerkers van persoonsgegevens zoals bedoeld onder de AVG. De iVRI-leveranciers (Cluster 1) verwerken enkel persoonsgegevens ten behoeve van de doelen die de wegbeheerder gelet op haar publieke taken heeft vastgesteld en vastgelegd. De iVRI-leveranciers (Cluster 1) hebben zelf géén doel en middelen vastgesteld en voeren enkel verwerkingen uit zoals vastgelegd in overeenkomsten met de wegbeheerder. Het is binnen deze verwerkersrelatie ook niet toegestaan dat iVRI-leveranciers (Cluster 1) de gegevens die zij in opdracht van de wegbeheerder verwerken verder verwerken voor eigen doeleinden. Voor de wegbeheerders is het dus zaak goede afspraken te maken met hun iVRI-leverancier(s).

Er moet om deze reden een verwerkersovereenkomst gesloten worden tussen de wegbeheerders en de iVRI-leveranciers (Cluster 1). Zowel met die van de TLC, de RIS als de ITS-applicatie, indien deze van verschillende leveranciers zijn afgenomen. Als een leverancier meerdere onderdelen levert, volstaat één verwerkersovereenkomst voor die geleverde onderdelen. Het is van groot belang dat wegbeheerders met iVRI-leveranciers in deze overeenkomsten afspreken dat iVRI-leveranciers de data niet voor andere doeleinden dan binnen de scope/opdracht van de wegbeheerder mag gebruiken. Daarnaast zal iedere wegbeheerder diens iVRI-leverancier(s) op de naleving hiervan ook periodiek moeten controleren.

Voor de service providers (Cluster 3) geldt dat zij met hun eigen cloud providers (Cluster 2) een verwerkersovereenkomst moeten sluiten. Indien een cloud provider (Cluster 2) of service provider (Cluster 3) diensten levert aan een professionele weggebruikersorganisatie, zoals de nood- en hulpdiensten, OV-bedrijven, of logistieke sector, zal met die organisaties ook een verwerkersovereenkomst moeten worden gesloten. De cloud provider (Cluster 2) of service provider (Cluster 3) is in die rol dan verwerker of sub-verwerker. Immers, het kan zijn dat naast informatie over het voertuig ook namen van chauffeurs bij de cloud provider (Cluster 2) en/of service provider (Cluster 3) worden verwerkt ten behoeve van het leveren van de dienst. Zeker indien dit primair ziet op een dienst waarmee voor de werkgever of opdrachtgever inzichtelijk is waar een bepaald voertuig, inclusief chauffeur, zich bevindt of heeft bevonden, ziet dit primair op het in opdracht verwerken van persoonsgegevens.

Deze keten maakt dat er een verwerkersovereenkomst gesloten dient te worden tussen:

- 1) de service providers (Cluster 3) en hun cloud providers (Cluster 2);
- 2) de service providers (Cluster 3) die opereren als leverancier van FMS-diensten ten behoeve van o.a. de logistieke sector en de professionele organisaties (werkgevers) van die weggebruikers;
- 3) de cloud providers (Cluster 2) die opereren als leverancier van diensten ten behoeve van nood- en hulpdiensten en OV-voertuigen en die diensten die bij hun zijn aangesloten;
- 4) de wegbeheerder en diens iVRI-leverancier(s) (Cluster 1).

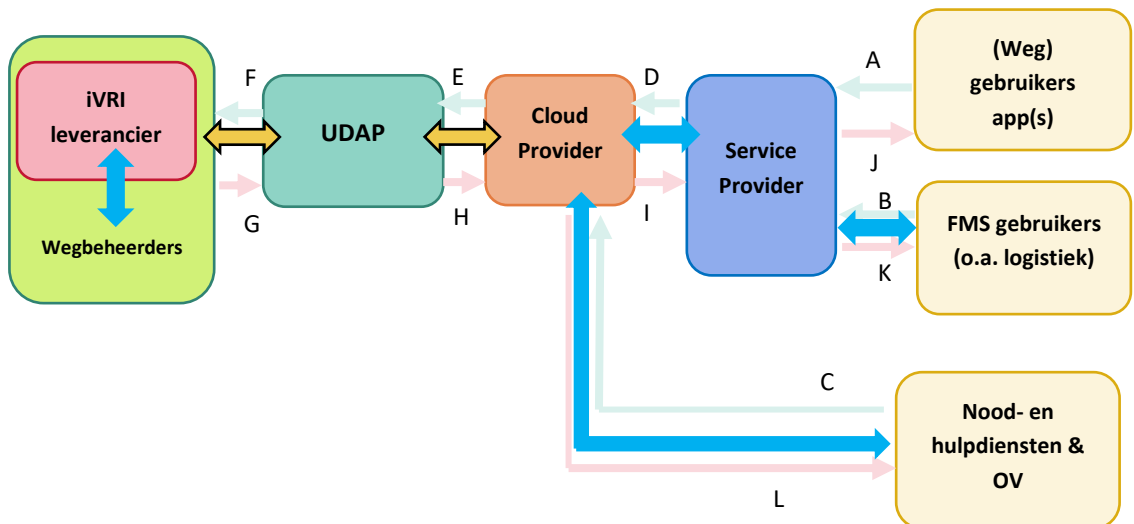
Dit is in de onderstaande afbeelding aangegeven met een **blauwe pijl**.

Let op: bij service providers (Cluster 3) en de weggebruiker die buiten FMS gebruik maakt van een app kan het zijn dat, wanneer het gebruik van de app voortvloeit uit een overeenkomst/abonnement tussen de service provider en de werk- of opdrachtgever van de eindgebruiker, er ook voor de werk- of opdrachtgever (meer) data inzichtelijk is. In het geval de werk- of opdrachtgever een abonnement heeft afgesloten met de service provider, zal ook een verwerkersovereenkomst tussen die service provider en werk- of opdrachtgever moeten worden gesloten.

Gelet op UDAP zal er tussen de volgende partijen een gegevensuitwisselingssovereenkomst moeten worden gesloten:

- 1) de wegbeheerders en UDAP; en
- 2) de cloud providers (Cluster 2) en UDAP.

Dit is hieronder aangegeven met een **oranje pijl**.



Figuur 7 Illustratie van de verwerkers in de dataketen van Talking Traffic.

Al de aangegeven verwerkerovereenkomsten zijn afgesloten op het moment dat een iVRI gekoppeld is aan UDAP en berichten daarvan ontvangt. Bewaking hierop vindt plaats vanuit het programma Talking Traffic onder verantwoordelijkheid van IenW. In UDAP is een filter aangebracht, zodanig dat uitsluitend data vanuit service providers (Cluster 3) en hun cloud providers (Cluster 2) aan iVRI-leveranciers en wegbeheerders wordt doorgegeven indien die

wegbeheerders en iVRI-leveranciers (Cluster 1) een verwerkersovereenkomst zijn overeengekomen.

Voor de verwerkersovereenkomsten tussen wegbeheerders en iVRI-leveranciers (Cluster 1) is een standaard verwerkersovereenkomst opgesteld. Sommige wegbeheerders en sommige iVRI-leveranciers hebben er voor gekozen om hierop zelf aanpassingen te maken. Daardoor is er sprake van een aanzienlijke diversiteit aan verwerkersovereenkomsten tussen wegbeheerders en iVRI-leveranciers. Inmiddels (1 augustus 2022) hebben circa 75 wegbeheerders in totaal 89 Verwerkersovereenkomsten afgesloten met hun iVRI-leveranciers.

Niet alle wegbeheerders zijn al gereed met het afsluiten van een verwerkersovereenkomsten met 'hun' iVRI-leverancier(s). Om te voorkomen dat data aan iVRI's wordt verstrekt vanuit UDAP zonder het bestaan van een getekende verwerkersovereenkomst, is in UDAP een zogenaamd CAM&SRM-filter ingebouwd. Dit filter werkt op basis van een 'white list'. Dit is een registratie van partijen op basis van specifieke vereisten. Op deze white list staan uitsluitend wegbeheerders die met al hun iVRI-leveranciers een wederzijds ondertekende verwerkersovereenkomst hebben afgesloten. Voor wegbeheerders die nog niet op de white list staan, garandeert het CAM&SRM-filter dat er naar de iVRI's van deze wegbeheerder géén CAM- en SRM-berichten worden gestuurd. SPaT en MAP berichten vanuit de iVRI richting cloud providers (Cluster 2) en service providers (Cluster 3) worden niet geblokkeerd door het CAM & SRM-filter, want deze berichten bevatten geen persoonsgegevens.

3.3 GRONDSLAG VERWERKING PERSOONSGEGEVENS

De AVG geeft duidelijk aan dat, om persoonsgegevens te mogen verwerken, er niet enkel een doel dient te zijn dat de verwerking noodzakelijk maakt. De verwerking dient ook gebaseerd te zijn op één van zes zogenaamde grondslagen, die zijn vastgelegd in artikel 6 AVG, om de rechtmatigheid van de verwerking vast te stellen.

3.3.1 Grondslag wegbeheerders

Eén van deze zes grondslagen betreft artikel 6 lid 1 sub e: *“de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen”*.

Deze taak in het kader van de uitoefening van het openbaar gezag, die aan een gemeente, provincie, waterschap en de Minister van Infrastructuur en Milieu (gemandateerd aan en uitgevoerd door Rijkswaterstaat) als wegbeheerder is opgedragen, vloeit voort uit de Wegenverkeerswet 1994.

De wegbeheerders zijn op grond van artikel 18 lid 2 Wegenverkeerswet 1994 bevoegd tot het nemen van verkeersbesluiten voor het verkeer op de wegen die onder hun beheer vallen. Aan plaatsing van verkeersregelininstallaties moet op grond van artikel 15 lid 2 Wegenverkeerswet 1994 altijd een verkeersbesluit vooraf gaan. Dit betekent dat enkel de wegbeheerders bevoegd zijn tot het plaatsen van een verkeersregelininstallatie én ook of dit een VRI of iVRI-installatie betreft. Daarbij moet het verkeersbesluit gebaseerd zijn op de doelen opgesomd onder artikel 2 Wegenverkeerswet 1994, namelijk:

- het verzekeren van de veiligheid op de weg;
- het beschermen van weggebruikers en hun passagiers;
- het in stand houden van de weg en het waarborgen van de bruikbaarheid daarvan;

- het zoveel mogelijk waarborgen van de vrijheid van het verkeer;
- het voorkomen van door verkeer veroorzaakte aantasting van het karakter of van de functie van objecten of gebieden;
- het bevorderen van doelmatig of zuinig energie verbruik.

Om meerdere van deze doelen te bevorderen c.q. te borgen, kan een wegbeheerder een verkeersbesluit nemen tot het plaatsten van een verkeersregelininstallatie, in dit geval een iVRI. Het kunnen registreren in de openbare ruimte van actueel weggebruik (aantallen, rijrichting, categorieën, tijdstippen, snelheden, voorrang) is door een wegbeheerder (of private partij die dit namens de wegbeheerder in opdracht uitvoert) in Nederland gemeengoed. Registratie van dergelijk weggebruik met digitale middelen, mits proportioneel en voorzien van deugdelijke maatregelen ter bescherming van de persoonlijke levenssfeer, valt binnen de grondslag die de wet heeft toegekend aan wegbeheerders.

3.3.2 Grondslag service providers (Cluster 3)

Service providers (Cluster 3) krijgen door het verwerken van gegevens inzicht in de context van het omringende, aankomende en/of verwachte verkeer van hun gebruikers. Zij brengen relevante informatie voor weggebruikers in kaart, zodat zij specifiek, op verzoek van de weggebruiker actueel advies op maat kunnen geven. De grondslag voor service providers (Cluster 3) is de volgende:

- Toestemming (AVG artikel 6 lid 1 sub a).

Toestemming dient *vrijelijk, specifiek, goed geïnformeerd en ondubbelzinnig* gegeven te worden. Gelet op de informatiedienst en het gebruik van de app moet de toestemming voorafgaand aan de verwerking worden verkregen. Dit betekent dus voorafgaand aan het versturen van bepaalde persoonsgegevens in de keten naar de uiteindelijke iVRI('s).

Vrijelijk

De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de verwerkingsverantwoordelijke verschillende doeleinden voor verwerking heeft samengevoegd en niet heeft getracht om voor elk doel afzonderlijke toestemming te krijgen, is er sprake van een gebrek aan vrijheid. Met andere woorden bepaalde elementen van vrijheid vallen samen met de eis dat de toestemming (ook) specifiek moet zijn voor het doel waarvoor de toestemming wordt gevraagd.

De toestemming is tevens pas 'vrij' gegeven indien deze niet voorwaardelijk wordt gehanteerd voor het leveren van de dienst. Gelet op artikel 7 lid 4 AVG mag 'toestemming' niet voorwaardelijk zijn voor het leveren van de overeengekomen diensten op basis van de overeenkomst of gebruiksvoorwaarden. Als toestemming is opgenomen als een niet-onderhandelbaar onderdeel van de voorwaarden, dan is de toestemming niet vrijelijk verleend en dus niet rechtsgeldig. De gebruiker moet namelijk de mogelijkheid hebben om voor specifieke diensten en de daarvoor benodigde gegevensverwerking die niet noodzakelijk zijn voor het gebruik van bijvoorbeeld de app te kunnen weigeren. Verder is er geen sprake van een bepaalde machtsverhouding tussen de service provider (Cluster 3) en eindgebruikers, wat een mogelijke vrijelijk gegeven toestemming in de weg zou kunnen staan.

Specifiek

Op het moment dat een individu ervoor kiest om gebruik te maken van een applicatie van een service provider (Cluster 3), wordt er door die service provider gewerkt met toestemming voor het verzamelen van bepaalde persoonsgegevens. Diverse service providers (Cluster 3) vragen middels het instemmen met hun privacy statement, instemming om de verplaatsingsgegevens van de app-gebruiker te gebruiken voor specifieke doeleinden. Daarnaast wordt bij het gebruik van de app gevraagd of de eindgebruiker toestemming geeft om de locatiegegevens van het device te delen met de service provider. Dit betreft een algemene toestemming voor het gebruik van de locatiegegevens voor het leveren van de diensten. Specifiek betekent specificeren welke gegevens gebruikt worden voor het leveren van welke dienst. Daarmee is zulke toestemming niet specifiek en voldoet deze toestemming niet aan het vereiste van artikel 7 AVG. Dit maakt dat een algemene toestemming in dit concrete geval niet rechtsgeldig is en de verdere verwerking van die gegevens niet rechtmatig is.

Geïnformeerd

Uit de AVG, en ook nader beschreven door de European Data Protection Board (EDPB) in haar Richtsnoeren over 'toestemming', volgt dat toestemming niet mag worden opgenomen in algemene voorwaarden, privacybepalingen of informatie die in juridisch jargon is geschreven. Ook is de 'toestemming' niet geldig als in algemene zin wordt ingestemd met de privacyverklaring of algemene (gebruiks)voorwaarden waar die specifieke verstrekking van verplaatsings- of locatiegegevens in is beschreven. Toestemming moet duidelijk en begrijpelijk zijn en ook te onderscheiden zijn van andere zaken.¹⁰ De verwerkingsverantwoordelijke moet een *duidelijke beschrijving* geven van het *specifieke* doel van de gegevensverwerking waarvoor toestemming wordt gevraagd. De eindgebruiker moet begrijpen en weten waarvoor deze specifiek toestemming geeft. Het toestemming geven middels een app zal gelet op de gebruikerservaring in gelaagdheid kunnen worden aangeboden. Essentieel is wel dat aan de vereisten voor een rechtsgeldige toestemming wordt voldaan. Dit betekent dat als bijvoorbeeld op het device (smartphone, tablet of geïntegreerd smart-navigatiesysteem) toestemming wordt gevraagd voor het delen van verplaatsingsgegevens met specifieke derden, minimaal wordt aangegeven voor welk doel de toestemming wordt gevraagd. Indien een service provider (Cluster 3) toestemming vraagt aan de eindgebruiker van de app, zal de toestemming voor het delen van de gepseudonimiseerde persoonsgegevens met uiteindelijk de iVRI van een wegbeheerder moeten aangeven waarvoor precies de toestemming wordt gevraagd. Wel kan middels gelaagde informatie worden doorverwezen naar de privacyverklaring of uitleg en toelichting elders. Deze informatie moet uiteraard voldoen aan de artikelen 13 en 14 AVG, zodat aan het recht op informatie wordt voldaan. Kortom, het louter instemmen met een privacyverklaring of algemene voorwaarden (of vergelijkbaar) voldoet niet aan de eisen van voldoende specifiek en goed geïnformeerd.

Ondubbelzinnig:

De toestemming moet worden verleend door middel van een actieve handeling of verklaring. Het vraagt dus om een opzettelijke handeling, zodat de eindgebruiker de toestemming ook bewust en weloverwogen geeft. Tevens moet het duidelijk zijn dat de eindgebruiker toestemming heeft verleend voor de specifieke verwerking.

Er zijn service providers (Cluster 3) die ten behoeve van prioriteitsfacilitering wel werken met een werkwijze en expliciete toestemming voor het delen van bepaalde persoonsgegevens in de iVRI-datasetten. Hierbij kan de werkgever of opdrachtgever een koppelcode sturen aan de chauffeur die vervolgens deze code moet accepteren. In dat geval behelst de toestemming een

¹⁰ EDPB Richtsnoeren "Toestemming", 05/2020, nr. 67.

actieve handeling van de chauffeur. Dit is een ondubbelzinnige actieve handeling. Let wel: de prioriteitsfacilitering zal in de regel efficiënt zijn met het oog op de logistieke keten, dus het primaire belang van de werk- of opdrachtgever. Deze data kan verder door een werk- of opdrachtgever ook voor andere doeleinden worden gebruikt, zoals controle van personeel of opdrachtnemers. Zodoende zal er niet snel sprake zijn van een vrijelijk gegeven toestemming. In deze arbeids- dan wel opdrachtgever/nemer relatie zal een toestemming voor de prioriteitsfacilitering ons inziens enkel geldig zijn indien de werkgever geen inzicht heeft in de data en resultaten die voor de prioriteitsfacilitering worden verwerkt. Of dit ook de werkwijze is, dan wel of er sprake is van een geldige toestemming zal door de individuele service provider (Cluster 3) en haar klanten moeten worden beoordeeld.

Mocht er onduidelijkheid ontstaan of er toestemming is verkregen, dan is het aan de verwerkingsverantwoordelijke om dit aan te tonen. Het zal in dit geval ook voorkomen dat informatiediensten voor verschillende verwerkingen toestemming vragen; het moet duidelijk zijn op welke *specifieke doelen en verwerkingen* de toestemming betrekking heeft. De betrokkene mag altijd zijn/haar toestemming intrekken. Als dit gebeurt, mogen er vanaf dat moment geen persoonsgegevens meer worden verwerkt.

Service providers (Cluster 3) hebben de plicht richting hun klanten/gebruikers zorgvuldig om te gaan met persoonsgegevens. Daarnaast kunnen service providers (Cluster 3) voor het overtreden van de privacy wetgeving forse boetes opgelegd krijgen vanuit de Autoriteit Persoonsgegevens. Daarom willen de service providers (Cluster 3) alleen hun data doorsturen aan wegbeheerders die een verwerkersovereenkomst hebben met hun iVRI-leverancier (Cluster 1) en is daartoe het CAM&SRM filter in UDAP geplaatst en ziet IenW als verantwoordelijke van UDAP toe op het aangaan van verwerkersovereenkomsten tussen de wegbeheerder en diens iVRI-leverancier(s).

Zonder verwerkersovereenkomst, en dus zonder dat CAM- en SRM-berichten naar een iVRI mogen worden gezonden, blijft een groot deel van het potentieel en daarmee het doel van een iVRI onbenut. Want zonder gebruik en doorgifte van CAM- en SRM-berichten zijn de Use Cases Prioriteren en Optimaliseren niet mogelijk en is de regeling van de iVRI onvoldoende aan te passen aan het steeds wisselende, actuele verkeersaanbod.

NB: Dankzij het CAM&SRM-filter kunnen iVRI's zonder enige impact op de privacy en AVG worden aangesloten op UDAP zodat SPaT en MAP data verstrekt wordt aan private derden. Deze bevatten immers uitsluitend signaalgegevens van lampen en topologische data van kruispunten en geen tot personen te herleiden kenmerken. Daarmee wordt het wel mogelijk om de Use Case Informeren aan weggebruikers beschikbaar te stellen. Want bij de Use Case Informeren zendt de iVRI alleen maar SPaT en MAP-data die niet persoons-gerelateerd is, maar ontvangt niets retour vanuit het private deel van de verdere keten.

Aan de andere kant begint de gegevensuitwisseling in de iVRI-dataketen met het rechtsgeldig toestemming vragen aan de klanten/gebruikers van de service providers (Cluster 3). Indien de toestemming daar niet rechtsgeldig is, zal de verdere verwerking van de gegevens in de dataketen ook niet rechtsgeldig zijn.

Gelet op de 'grondslag' toestemming die door de service providers (Cluster 3) wordt gebruikt, voldoet deze op meerdere onderdelen nog niet aan de eisen van rechtsgeldige toestemming. De scope van deze ketenbrede PIA vereist dat iedere service provider (Cluster 3) individueel, als zelfstandig verwerkingsverantwoordelijke moet beoordelen of de toestemming die zij van haar

eindgebruikers vraagt daadwerkelijk voldoet aan de eisen van een vrijelijk, specifiek, goed geïnformeerde en ondubbelzinnige toestemming.

3.4 PROPORTIONALITEIT EN SUBSIDIARITEIT

Naast het feit dat een verwerking gebaseerd dient te zijn op één van de grondslagen zoals genoemd in de AVG, moet zij noodzakelijk en evenredig zijn. Hierbij moet worden afgewogen of de (eventuele) inbreuk op de persoonlijke levenssfeer en bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staan tot de verwerkingsdoeleinden, en of de verwerkingsdoeleinden niet in alle redelijkheid op een andere, voor de betrokkenen minder nadelige wijze, kunnen worden verwezenlijkt.

Meer inhoudelijk is de vraag of de verwerking van persoonsgegevens in verhouding staat tot de doelen. In de literatuur over dit soort toetsingen wordt expliciet aangegeven dat de dringendheid van het maatschappelijk belang hier een belangrijke indicator voor is.¹¹ Het is aannemelijk, zo niet evident, dat bijvoorbeeld het prioriteit geven aan nood- en hulpdiensten om zo te voorkomen dat deze (met doorgaans hoge rijsnelheden) rood licht moeten negeren, een positieve bijdrage levert aan de verkeersveiligheid. Idem voor het prioriteit kunnen geven aan vervoer van gevaarlijke stoffen en/of het bevorderen dat OV-voertuigen volgens de dienstregeling hun maatschappelijke functie kunnen vervullen. Ook is het aannemelijk dat het prioriteit kunnen geven aan openbaar vervoersdiensten bijdraagt aan een voor reizigers aantrekkelijker openbaar vervoerdienst en zo aan de milieudoelstellingen van de wegbeheerders, die ook voortvloeien uit hun publieke taken op dit terrein. Het voorkomen van onnodig stoppen en optrekken van voertuigen middels individuele informatieverstrekking aan weggebruikers bevordert eveneens de milieudoelstellingen. En efficiënte en continu optimaliserende verkeersregeling die rekening houdt met het actuele verkeersaanbod, doet dit evenzeer. Zie ook de aanleidingen voor het Innovatiepartnerschap zoals deze in de inleiding van dit document zijn weergegeven.

Nadere toelichting op 'dringendheid van het maatschappelijk belang' voor het gebruiken van iVRI's door wegbeheerders

Redenen voor wegbeheerders om iVRI's te realiseren en deze aan te sluiten op de dataketen van Talking Traffic zijn onder andere:

- Verkorten van de reistijd voor openbaar vervoer en verbeteren van stiptheid en regelmaat van de dienstregeling;
- Beperken van het aantal stops van vrachtverkeer en daarmee het beperken van uitstoot en verbeteren van leefbaarheid;
- Verhogen van verkeersveiligheid ten goede van nood- en hulpdiensten bij het passeren van met iVRI's geregeld kruispunten.
- Optimaliseren van de verkeersafwikkeling door verbeterd presteren van kruispunten past bij de doelstelling van het voorkomen van door verkeer veroorzaakte aantasting van het karakter of van de functie van objecten of gebieden;

Deze diensten worden mogelijk doordat zowel de iVRI als de (doelgroep)voertuigen zijn verbonden met elkaar en zo data kunnen uitwisselen. Hierdoor 'zien' iVRI's deze doelgroepen veel eerder en kunnen zij veel beter en vol-continu hun regelingen hierop aanpassen. Dit is niet mogelijk met traditionele VRI's die worden geregeld op basis van informatie uit lusedetectoren direct rondom een kruispunt met een

¹¹ Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

verkeerslicht. De lusdetectoren zijn geplaatst op een beperkte afstand van het kruispunt, waardoor aankomende voertuigen gegeven hun rijsnelheid pas relatief laat kunnen worden gedetecteerd. Ook zijn deze in de praktijk kwetsbaar gebleken voor weersomstandigheden en slijtage, waardoor deze veelvuldig niet of onvoldoende detectie van aankomende voertuigen opleveren. Het is financieel en operationeel ondoenlijk om op alle wegen lusdetectoren aan te brengen en te onderhouden ten behoeve van een adequate verkeersdetectie.

Bovendien kan, op termijn, met een voldoende penetratiegraad van deze diensten, in ieder geval een deel van de lusdetectoren mogelijk verdwijnen, waardoor voor wegbeheerders aanzienlijke kostenbesparingen mogelijk worden. Ook zijn dan specifieke technische oplossingen in VRI's, zoals KAR, VETAG en VECOM, niet meer nodig, hetgeen ook kosten bespaart voor realisatie en beheer.

Het doel van de verwerkingen van de wegbeheerders is derhalve het beter en kostenefficiënter – dat wil zeggen kosten in relatie tot baten – realiseren van maatschappelijke en beleidsmatige doelstellingen ten aanzien van bereikbaarheid, veiligheid, duurzaamheid en leefbaarheid.

De CAM- en SRM-berichten die door de iVRI leveranciers (Cluster 1) worden verwerkt, onder verantwoordelijkheid van de wegbeheerder, zouden tot op zekere hoogte inbreuk kunnen maken op de privacy rechten van betrokkenen. Echter, de CAM-berichten vanuit cloud providers (Cluster 2) aan UDAP en verder richting iVRI, mogen enkel worden verstuurd vanuit weggebruikers/klanten die daadwerkelijk toestemming hebben gegeven voor het gebruik van die gegevens, voor dat specifieke doel. Zolang een wegbeheerder niet de pseudonimisering van de StationID doorbreekt, levert de Talking Traffic keten geen inbreuk op op de rechten en vrijheden van de betrokkenen. Als de wegbeheerder wel de pseudonimisering van de StationID doorbreekt, levert dat wel een grote inbreuk op.

De proportionaliteit van de inbreuk hangt ook samen met de bewaartermijnen van deze data door de verwerkingsverantwoordelijke. De CAM-berichten die bij de iVRI binnenkomen, zijn voorzien van een tijdelijk StationID. Dat StationID (de pseudo-identiteit bestaande uit een willekeurige cijfercombinatie die automatisch 'at rondom' wordt gegeneerd) wordt weer verwijderd nadat het voertuig de stopstreep op dat kruispunt is gepasseerd. De StationID verandert per kruispuntgebied en wordt niet opgeslagen. Deze wordt alleen gebruikt en doorgegeven vanuit cloud providers (Cluster 2) aan UDAP en de iVRI-leveranciers om op dat specifieke moment, op die specifieke kruispuntlocatie, de optimale verkeersafwikkeling te registreren. Vervolgens verdwijnen de berichten weer. Individuele wegbeheerders leggen dit vast in hun verwerkersovereenkomsten en dienen periodiek de nakoming hiervan te controleren. Voor zover hiermee al inbreuk zou worden gedaan op de privacy van betrokkenen, weegt dit niet op tegen het maatschappelijke belang op veiligere, duurzame en efficiëntere verkeersdoorstroming. En zijn waarborgen vastgelegd in de verwerkersovereenkomsten tussen de organisaties in de keten.

SRM-berichten bevatten een tijdelijk unieke identifier van het voertuig waarvoor prioriteit wordt aangevraagd. Ook deze berichten worden enkel gebruikt op een specifiek moment in dat specifieke kruispuntgebied en worden vervolgens weer verwijderd (net als StationID).

Zoals eerder aangegeven worden CAM-berichten door UDAP en de ontvangende iVRI-leverancier direct verwijderd, nadat het voertuig met die StationID de stopstreep op dat kruispunt is gepasseerd. Ditzelfde geldt voor SRM-berichten, deze berichten worden niet opgeslagen in UDAP of door een iVRI-leverancier (Cluster 1).

Dit privacymodel hangt op de correcte uitvoering van de pseudonimisering van de StationID en de afwezigheid van andere gegevens die alsnog identificerend kunnen werken. Verder heeft

een wegbeheerder de mogelijkheid om de data dusdanig te combineren met andere data (bijv. camerabeelden) waardoor een natuurlijk persoon herleidbaar zou kunnen zijn.

Dit afzettende tegen het doel om de verkeersveiligheid te verhogen, leefbaarheid en duurzaamheid te verbeteren en de verkeersstromen efficiënter te regelen, is de inbreuk op de privacy, voor zover daar sprake van zou zijn, mits er sprake is van correct gebruik van het tijdelijke StationID's, proportioneel, mits uiteraard ook tussen wegbeheerders en iVRI-leveranciers deugdelijk vastgelegd conform de technische specificaties en verantwoordelijkheidsverdeling van de Talking Traffic architectuur (zie Figuur 2 Het Innovatiepartnerschap Talking Traffic op basis van de opgeleverde documentatie”).

Ten behoeve van de ketenbrede PIA Talking Traffic is de scope beperkt tot de gegevensuitwisseling respectievelijk overdracht tussen de service providers (Cluster 3) en cloud providers (Cluster 2) en iVRI's van de wegbeheerders middels UDAP, en vice versa. Een belangrijke kanttekening is dat:

1. Wegbeheerders gelet op hun publieke taken over meer data kunnen beschikken. De StationID's zijn gedurende de maximaal vijf minuten dat ze gelijk blijven, te herleiden tot personen. Door die korte tijd, is het risico dat een StationID in de praktijk voor de wegbeheerder daadwerkelijk herleidbaar is, zeer beperkt. Indien de wegbeheerder specifiek StationID's verder wil gebruiken en in strijd met de doeleinden van gebruik (en dus AVG) ook elders opslaat, zou zij de StationID en overige informatie uit die berichten met andere voor haar beschikbare data kunnen combineren waardoor de StationID herleidbaar kan zijn. Denk hierbij aan het gegeven dat de wegbeheerder daarnaast ook kan beschikken over andere data, zoals camera's.
In ieder geval moet voor verder gebruik van data – al dan niet in geaggregeerde vorm – door een wegbeheerder altijd worden onderzocht of die (verdere) verwerking, waaronder dus ook het combineren van data, rechtmatig is. Dit vraagt een individuele en afzonderlijke beoordeling door die wegbeheerder.
2. UDAP vormt een scheiding tussen de wegbeheerders (Cluster 1) en de cloud providers (Cluster 2) en de service providers (Cluster 3). De iVRI-leveranciers (Cluster 1) treden op als verwerker voor wegbeheerder. De cloud providers en de service providers zijn zelfstandig verantwoordelijk. Als een iVRI-leverancier ook actief is als cloud provider en/of als service provider, dan kan de leverancier buiten de UDAP om een communicatie stroom tussen Cluster 1 enerzijds en Cluster 2/3 anderzijds opzetten. Daardoor kan de wegbeheerder de controle over de gegevensstromen verliezen. Dus als een leverancier zowel actief is als leverancier van iVRI's en actief is als cloud provider en service provider, dus als een leverancier actief is in Clusters 1, 2 en 3, dan dient deze leverancier de gegevens van de iVRI systemen (Cluster 1) strikt gescheiden te houden van de clouddiensten en de op de eindgebruiker gerichte service (Cluster 2 en 3).

3.5 VERANTWOORDELIJKHEDEN PARTIJEN TALKING TRAFFIC KETEN

Binnen de dataketen van Talking Traffic

Algemeen

Vanuit de aanbesteding- en contractstukken van Talking Traffic zijn er eisen gesteld aan de iVRI ten aanzien van privacy en security, waaraan partijen zich dienen te houden en waarop gecontroleerd kan worden. Zo zijn alle private Talking Traffic partners ge-audit in opdracht van het ministerie van Infrastructuur en Waterstaat en zal dit ook periodiek worden herhaald. Zij zal blijven monitoren dat deze partijen aan hun (wettelijke) verplichtingen voldoen. Sowieso zijn alle ketenpartners zelf verantwoordelijk om te voldoen aan de vigerende wet- en regelgeving, ook op het gebied van privacy en security.

Alle deelnemende overheden en bedrijven zijn als ketenpartners vertegenwoordigd in de governance structuur bestaande uit:

1. De werkgroep Exploitatie (publiek-privaat, de inhoudelijk deskundigen van organisaties die deelnemen in de Talking Traffic dataketen).
2. De werkgroep Intelligente Kruispunten (publiek, de iVRI-deskundigen van wegbeheerders).
3. De Council (publiek-privaat, de directeuren van organisaties die deelnemen in de Talking Traffic dataketen).

Specifiek ten aanzien van de Talking Traffic dataketen

Doordat niet alle cloud providers (Cluster 2) en service providers (Cluster 3) een strikte scheiding hebben tussen de onderlinge datastromen, worden soms ook functionaliteiten die bij een cloud provider horen uitgevoerd door de service provider. Daardoor kan er onduidelijk ontstaan over waar de verantwoordelijkheid, bijvoorbeeld voor het samenstellen van de SRM berichten, ligt. Het is van belang dat de functie die cloud providers (Cluster 2) hebben bij het bepalen van de prioriteit en het samenstellen en verzenden van SRM berichten gehandhaafd blijft.

Het privacymodel van Talking Traffic valt of staat bij het niet herleidbaar zijn van het StationID. Uit het technische onderzoek blijkt dat Talking Traffic er niet op kan vertrouwen dat de vanuit Cluster 2 aangeleverde CAM en SRM berichten een correct gegenereerde StationID hebben en niet via andere gegevens heridentificeerbaar zijn. Het is aan alle op UDAP aangesloten cloud providers (Cluster 2) dat dit op correcte wijze plaatsvindt. Om de integriteit van de keten (verder) te waarborgen, moet I&W:

- De berichten die door UDAP doorgegeven worden, controleren op de correctheid van de StationID's en de aanwezige gegevens.
- Handhavend optreden tegen partijen die incorrecte CAM en SRM berichten verzenden.

Het is aan te raden om in de iVRI standaarden explicieter te maken aan welke regels de implementaties aan moeten voldoen wat betreft privacy.

Controle op nakoming

Het vastleggen van concrete en specifieke afspraken in bilaterale overeenkomsten is een goed begin. Toetsing op nakoming van die afspraken is eveneens vastgelegd in die overeenkomsten. Onvoldoende nakoming heeft ook consequenties. In voorkomende gevallen kunnen die consequenties leiden tot in gebreke stelling, aansprakelijkstelling en schadeverhaal. Dit is uiteraard afhankelijk van het geconstateerde tekort in nakoming, de ernst en betekenis/impact hiervan als ook de verantwoordelijkheid van de betreffende partij.

Daarnaast heeft IenW het recht om zelf, of door haar aangewezen derden controles periodiek uit te voeren. Hiervan is gebruik gemaakt door Audits en Penetratietesten uit te voeren om de deugdelijkheid van databescherming door de bedrijven in de keten vast te stellen. Die uitgevoerde testen en audits hebben tot op heden geen aanleiding gegeven tot contractuele maatregelen vanuit IenW.

Buiten de dataketen van Talking Traffic

Algemeen

Ook activiteiten van wegbeheerders en private partijen buiten de dataketen vragen aandacht vanuit privacy en security. Denk bijvoorbeeld aan V-Log gegevens: wie heeft er toegang tot deze data, met wie worden deze data gedeeld en zijn daar afdoende afspraken over gemaakt? Worden er wellicht gegevens gedeeld met of via het NDW? Zijn er goede afspraken gemaakt tussen wegbeheerders en de beheerder van hun VRI-beheercentrale? Hetzelfde geldt ook voor eventuele camera's die op, bij of naast een kruispunt hangen om de verkeersstromen te monitoren en efficiënter en veiliger te laten verlopen. Welke organisatorische en technische maatregelen zijn er genomen om de verwerkingen zorgvuldig uit te voeren? Dit zijn aandachtspunten voor wegbeheerders en private partijen die veelal buiten de verantwoordelijkheid van het programma Talking Traffic liggen, maar ook aandacht blijven vragen.

Het verdere gebruik of combineren van data uit de Talking Traffic keten en data van buiten

Zowel de cloud providers (Cluster 2) als de iVRI-leveranciers (Cluster 1) mogen geen van de binnen de Talking Traffic verkregen data verwerken voor eigen doeleinden. Dit omdat beide partijen uitsluitend optreden als verwerker. Enerzijds de service providers (Cluster 3) en cloud providers (Cluster 2) als verwerker en anderzijds de wegbeheerders en haar iVRI-leveranciers (Cluster 1) als verwerker.

De publieke keten: wegbeheerders en hun iVRI-leveranciers

Het is van groot belang dat wegbeheerders de CAM en SRM data die zij middels UDAP ontvangen enkel voor het doel van het optimaliseren van de regeling van hun iVRI's, respectievelijk de invulling van de prioriteitsfacilitering gebruiken. De service providers (Cluster 3) verstrekken immers die data via cloud providers (Cluster 2) en UDAP naar de iVRI's van wegbeheerders op basis van toestemming van hun eindgebruikers. Dit betekent voor wegbeheerders dus ook, dat zij die data buiten die scope van verleende toestemming (optimaliseren van de regeling van iVRI's en invulling van de prioriteitsfacilitering) niet zomaar voor andere doeleinden mogen gebruiken. Iedere wegbeheerder moet er dus voor waken de CAM- en SRM berichten enkel te verwerken binnen de wettelijke kaders (in het bijzonder de Wegenverkeerswet, AVG en relevante wet- en regelgeving). Er moet dus voorkomen worden dat de wegbeheerder (of diens iVRI-leverancier) de CAM-, en SRM-berichten verrijkt met data uit andere databases (zoals camera's of andere persoonsgegevens). Het gevolg kan zijn dat de 'niet-herleidbare' data uit de CAM- en SRM berichten voor de wegbeheerder dan alsnog herleidbaar zijn tot personen.

Kortom, als een wegbeheerder zich zuiver houdt aan dit op toe- of instemming gerichte gebruik van de CAM en SRM berichten ten behoeve van optimaliseren van de regeling van iVRI's en invulling van de prioriteitsfacilitering middels iVRI's, zijn de persoonsgegevens voor de wegbeheerder niet herleidbaar tot personen. Belangrijk is daarbij wel dat de gecontracteerde iVRI-leveranciers (Cluster 1) zich strikt houden aan de instructies van de wegbeheerder op basis van de verwerkersovereenkomst én de data niet voor andere doeleinden gebruiken of (kunnen) combineren met andere data. Dit met name met het oog op de diverse marktpartijen die zowel diensten aanbieden als iVRI leverancier (Cluster 1), cloud provider (Cluster 2) en/of service provider (Cluster 3). Met andere woorden: voor de zuivere rol als verwerker mag het ook voor de iVRI leveranciers (Cluster 1) niet mogelijk zijn om op basis van de voor hen beschikbare data deze alsnog nog tot een persoon te kunnen herleiden.

Het private deel van de keten: de cloud providers (Cluster 2) en service providers (Cluster 3)

Aan de andere kant ontvangen de service providers (Cluster 3) (middels de cloud providers (Cluster 2)) de MAP, SPaT en SSM data van wegbeheerders middels UDAP. De wijze waarop zij deze data vervolgens gebruiken richting hun eindgebruikers is in eerste instantie gericht op de informatievoorziening en prioriteitsfacilitering. En moet voortvloeien uit de toestemming die zij

in eerste instantie hebben verkregen van hun eindgebruiker voor het verstrekken van de CAM en SRM berichten naar de iVRI's van wegbeheerders. De service providers (Cluster 3) kunnen de data ook verder gebruiken voor de door hun aangeboden diensten, echter is het de verantwoordelijkheid van iedere individuele service provider (Cluster 3) dat hierbij wordt gehandeld conform de AVG, relevante wet- en regelgeving en afspraken met, dan wel met toestemming van de eindgebruikers. Dit handelen conform de AVG, relevante wet- en regelgeving geldt ook als een service provider diensten aanbiedt aan professionele weggebruikers of als een service provider geïntegreerd is met een cloud provider. In een dergelijk geval zal doorgaans gerechtvaardigd belang de grondslag zijn. Denk hierbij aan de applicatie van Ambulancezorg Nederland die geleverd wordt door en in beheer is bij Cluster 2 partij Be-Mobile.

Nieuwe bedrijven die willen aansluiten

Voor nieuwe partijen (anderen dan degenen die krachtens het resultaat van de EU aanbesteding van Talking Traffic in de periode 2017 tot en met 2020 in een contractrelatie werkten met lenW) die data willen uitwisselen binnen de Talking Traffic dataketen, is een uitgebreid dossier "Aansluiten en Toetreden" opgesteld waarin alle eisen, specificaties, standaarden en verantwoordelijkheden voor nieuwe ketenpartners zijn vastgelegd. Indien 'nieuwe' partijen gebruik wensen te maken van de mogelijkheid onderdeel te worden van deze dataketen, dan dienen ze zich aan dezelfde eisen te conformeren als die welke gelden voor de bestaande ketenpartners en aan te tonen dat ze dit doen resp. op welke wijze. Pas nadat die conformiteit is aangetoond kan data met andere ketenpartners worden uitgewisseld, bijvoorbeeld middels aansluiting op UDAP. Hiermee wordt gebruik (ook op straat) en de kwaliteit (inclusief bescherming van privacy en security) bewaakt en geborgd.

Data Protection Impact Assessment DPIA

Een Data Protection Impact Assessment (DPIA), ook wel Privacy Impact Analyse (PIA) of Gegevensbeschermingseffectbeoordeling (GEB) genoemd, is een onderzoek naar de gevolgen van een bepaalde verwerking of verwerkingen van persoonsgegevens op de privacy. Het is een instrument dat bedoeld is om op een systematische wijze in kaart te brengen welke data wordt verwerkt, wie dat doet, met welke grondslag, op welke wijze en welke risico's die verwerkingen met zich meebrengen. Op basis van de uitkomsten van een DPIA kan een organisatie vervolgens maatregelen nemen om die risico's te beperken.

Een DPIA is vanuit de AVG verplicht als er sprake is van hoog risicodragende verwerkingen. Dit kan bijvoorbeeld het geval zijn als het gaat om een groot aantal betrokkenen, maar ook als er veel persoonsgegevens per betrokkene worden verwerkt of als het gaat om bijzondere of gevoelige persoonsgegevens zoals medische of financiële gegevens.

Het is aan elke afzonderlijke organisatie die deelneemt aan de dataketen van Talking Traffic om zelf de afweging te maken een eigen DPIA uit te voeren voor het eigen handelen binnen deze dataketen. Dit geldt voor zowel overheden als voor bedrijven. lenW kan niet voor deze partijen besluiten of een DPIA al dan niet nodig is voor hun rol binnen Talking Traffic. Alleen al omdat elke partij zelf de eigen wijze kiest waarop zij intern hun eigen organisatie en binnen hun eigen producten het verwerken van data hebben georganiseerd. In het algemeen geldt ten aanzien van de wettelijke verplichtingen vanuit de AVG dat bij twijfel beter kan worden gekozen om wél zelf een DPIA uit te voeren. In alle gevallen zijn en blijven een afzonderlijke overheid en een individueel bedrijf zelf verantwoordelijk voor deze keuze, voor (de correctheid van) de uitvoering van de DPIA en voor het zelf nemen van eigen mitigerende maatregelen. lenW heeft echter wel in de bilaterale overeenkomsten nadrukkelijk opgenomen dat iedere ketenpartner

te allen tijde dient te blijven voldoen aan de geldende wet- en regelgeving, als ook het recht om hierop naar eigen behoefte te kunnen toetsen. Eveneens zijn aanzienlijke schadevergoedingen bedongen indien blijkt dat hieraan onvoldoende invulling wordt gegeven.

Vanuit de AVG is een 'ketenbrede PIA' geen wettelijk instrument en daarmee niet noodzakelijk. Het doel van een dergelijke ketenbrede analyse zou zijn om voor de gehele keten en op het niveau van de keten op een systematische wijze in kaart te brengen welke data wordt verwerkt, wie dat doet, met welke grondslag, op welke wijze en welke risico's die verwerkingen met zich meebrengen. Met het voorliggende document heeft lenW dit in kaart gebracht.

Eigen wettelijke verantwoordelijkheden

Alle partijen binnen de Talking Traffic keten zijn ook zelf wettelijk verantwoordelijk voor het sluiten van verwerkersovereenkomsten met alle verwerkingsverantwoordelijken/verwerkers waarvoor zij persoonsgegevens verwerken, of door wie zij persoonsgegevens laten verwerken. Zij dienen zelf onderling afdoende afspraken te maken om ervoor te zorgen dat de persoonsgegevens op zorgvuldige manier worden verwerkt en dit voldoet aan de AVG. Het is daarnaast de verantwoordelijkheid van de verwerkingsverantwoordelijke om de door haar te contracteren of gecontracteerde partijen periodiek te beoordelen of deze voldoen aan de AVG. De verwerkingsverantwoordelijke moet immers waarborgen dat de gegevensverwerking door de verwerker binnen de gestelde wettelijke kaders kan en blijft voldoen aan de AVG. Met name gelet op de privacy en rechten van de betrokkene (eindgebruikers).

Er is een voorbeeld verwerkersovereenkomst beschikbaar die elke wegbeheerder kan gebruiken. Wegbeheerders kunnen ook gebruikmaken van een 'Handreiking AVG voor Wegbeheerders'. Hierin staat in een aantal stappen uitgelegd wat een wegbeheerder moet regelen om te voldoen aan de wettelijke eisen ten aanzien van privacy. Beide documenten zijn beschikbaar op de [CROW-portal iVRI](#).

3.6 Risico's en te treffen maatregelen

Uit de analyse van de ketenbrede PIA Talking Traffic 2022 zijn diverse risico's gebleken waar de betrokken partijen maatregelen voor moeten treffen, willen zij gelet op privacy en security (blijven) voldoen aan de AVG. Hieronder worden de belangrijkste risico's in de dataketen inclusief de voorstellen voor maatregelen weergegeven:

Risico	Plaats in de keten	Impact	Beheersmaatregel	Verantwoordelijke
1. De toestemming voor de verwerking en verstrekking van de CAM- en SRM berichten door de service providers voldoet niet aan de eisen van de AVG.	Cluster 3 partijen	Groot: indien de toestemming niet voldoet aan de AVG betekent dit dat de verdere verwerking en verstrekking in de dataketen ook niet rechtmatig is. Dit is een overtreding van de AVG.	De Cluster 3 partijen dienen op de juiste wijze te zorgen voor het vragen en verkrijgen van toestemming zodat wordt voldaan aan de AVG.	Cluster 3 partijen
2. Wegbeheerder ontvangt niet-gepseudonimiseerde data uit het private domein, bijvoorbeeld door extra velden in de CAM berichten.	Wegbeheerder	Groot: want de wegbeheerder heeft voor het functioneren van de iVRI's en dus haar doeleinden géén persoonsgegevens nodig. Dit is een overtreding van de AVG.	Deugdelijke vastlegging van verplichtingen en beperking data-ontvangst en verwerking in Verwerkersovereenkomst met iVRI-leverancier.	Wegbeheerder
3. UDAP geeft niet-gepseudonimiseerde data door aan iVRI leverancier, bijvoorbeeld door extra velden in CAM berichten.	UDAP onder contract met lenW	Medium: overtreding AVG, echter veroorzaakt door niet-correcte naleving van doorgifte CAM berichten door Cluster 2 partijen.	Monitoring op de aanwezigheid van extra velden in CAM berichten.	UDAP uitvoerder onder verantwoordelijkheid lenW

4. iVRI-leverancier bewaart StationID's.	iVRI-leverancier in Cluster 1 onder contract met diens wegbeheerder	Groot: reconstructie van natuurlijke personen in combinatie met andere detectiesystemen zorgt voor het overtreden van de AVG.	Wegbeheerders leggen deugdelijk in de verwerkersovereenkomst met iVRI-leverancier verplichtingen en beperking data-ontvangst en verwerking vast, inclusief verplichting tot vernietiging StationID's.	Wegbeheerder
5. Wegbeheerder gebruikt StationID's voor andere doeleinden dan iVRI-regeling.	Wegbeheerder	Groot: want wegbeheerder treedt hiermee buiten haar doelbinding en heeft op die wijze onvoldoende de proportionaliteit geborgd. Wegbeheerder overtreedt hiermee de AVG door de data voor andere doeleinden te gebruiken. iVRI-leverancier overtreedt AVG door data voor andere doeleinden te laten gebruiken door diens opdrachtgever.	Wegbeheerders leggen deugdelijk in de verwerkersovereenkomst met iVRI-leverancier verplichtingen en beperking data-ontvangst en verwerking vast, inclusief verplichting tot vernietiging StationID's.	Wegbeheerder iVRI leverancier
6. De iVRI-leverancier heeft toegang tot data uit het private domein waardoor de informatie (indirect voor wegbeheerder) herleidbaar kan zijn tot personen	Wegbeheerder	Groot: hierdoor acteert de iVRI-leverancier niet als verwerker van de wegbeheerder. De iVRI-leverancier kan die data (her)gebruiken voor andere doeleinden. En de wegbeheerder kan (indirect) toegang hebben tot data waardoor herleidbaarheid mogelijk is. Overtreding van de AVG.	Vastleggen dat communicatie tussen Cluster 1 en Cluster 2 en 3 alleen via UDAP mag lopen.	iVRI-leveranciers en Wegbeheerders
7. Partijen in Cluster 2 en/of Cluster 3 gebruiken data anders dan waarvoor gebruikstoestemming is verleend door de klant	Private partijen	Groot: want overtreding AVG gelet niet voldoen aan de vereisten voor een rechtsgeldige toestemming (als grondslag voor de rechtmatige verwerking van de data).	Blijvende kennisopbouw en compliance borging bij private partijen	Cluster 2 en 3 partijen

8. Cluster 2 en 3 partijen hanteren niet op de juiste wijze pseudonimisering voor tijdelijke pseudo-ID's ten behoeve van doorgifte middels UDAP aan wegbeheerder	Private partijen	Groot: want kans op niet noodzakelijke herleidbaarheid van personen bij wegbeheerder (iVRI-leverancier). Overtreding AVG.	Monitoren op correctheid pseudo ID's.	UDAP uitvoerder onder verantwoordelijkheid van lenW
9. Onjuiste verwerkersrol en -overeenkomst tussen partijen en lenW gelet op UDAP	lenW, Cluster 2 en wegbeheerders	Medium: want voor UDAP (lenW) is de verkeerde rol bepaald en zodoende zijn door partijen ook de verkeerde verplichtingen onder de AVG aangegaan.	Sluiten van een gegevensuitwisselingsovereenkomst tussen wegbeheerders en lenW (UDAP) enerzijds, en sluiten gegevensuitwisselingsovereenkomst tussen Cluster 2 partijen en lenW (UDAP) anderszijds. En beëindigen verwerkersovereenkomst tussen UDAP en publieke respectievelijk private partijen	lenW, wegbeheerders en Cluster 2 partijen



DE
IVRI



Bijlage 1: gemeten effecten

<https://publications.dutchmobilityinnovations.com/november-2019#!/talking-traffic-hoe-staat-het-met-de-ivri>

In het artikel in bovenstaande link staan meerdere resultaten geformuleerd in de paragraaf 'Eerste resultaten' (tweede helft van het artikel). Dit betreft uiteraard een momentopname van November 2019. Naar verwachting in mei/juni 2020 zullen aanvullende evaluatiegegevens beschikbaar komen. Daarbij dient opgemerkt te worden dat de verkeerskundige effecten zullen blijven variëren naar locatie, traject, verkeerssamenstelling, tijdstip en beleidsprioriteiten van de individuele wegbeheerder.

In mei 2020 betrof de omvang van actieve gebruikers op landelijke schaal ca. 1,7 miljoen. Daarvan ontvangen ruim 600.000 gebruikers inmiddels iVRI-informatie uit ruim 450 iVRI's in Nederland.

Bijlage 2: technische analyse per service provider (Cluster 3)

Inleiding

De service providers (Cluster 3) leveren mobiliteitsapps die met cloud providers (Cluster 2) communiceren. Dit kan via het standaard berichtenformaat van de iVRI standaarden of via een eigen interface. De cloud providers (Cluster 2) zorgen vervolgens voor de communicatie met de iVRI's (Cluster 1). Onder de iVRI standaarden stuurt een service provider (Cluster 3) CAM berichten (met ondermeer de actuele positie, snelheid en rijrichting van het voertuig) naar diens cloud provider (Cluster 2).

Het aanvragen van een prioriteitsfacilitering, de SRM berichten, wordt in sommige gevallen door de cloudprovider (Cluster 2) verzorgd en in sommige gevallen door de serviceprovider (Cluster 3). In antwoord op een verzonden SRM bericht ontvangt de cloud provider (Cluster 2) via UDAP vanuit die iVRI (Cluster 1) een SSM bericht, en geeft dit door aan de service provider (Cluster 3) ter aflevering in het juiste voertuig. In de nabije toekomst kan deze berichtenstroom worden aangevuld met DENM berichten (omstandigheden op weg/kruising) en IVI berichten (informatie om te tonen in de auto).

De typische architectuur voor een service provider (Cluster 3) is dat deze een app heeft draaien op een mobiel apparaat van de weggebruiker. Die app maakt dan via een proprietary protocol verbinding met de eigen backend. De eigen backend heeft vervolgens interface welke volgens de Talking Traffic standaarden communiceert met de cloud provider (Cluster 2). En die communiceert via UDAP met de iVRI's (Cluster 1).

Aan service providers (Cluster 3) zijn een aantal specifieke privacyrisico's verbonden:

1. De ID's die een service provider (Cluster 3) naar een cloud provider (Cluster 2) stuurt, kunnen het mogelijk maken om een voertuig te volgen. Dit treedt op als de ID's over een lange periode hetzelfde zijn of als de ID's voorspelbaar zijn.
2. De route segments die een service provider (Cluster 3) naar een cloud provider (Cluster 2) stuurt, kunnen het mogelijk maken om een voertuig te volgen. Dit treedt op als de route segments te lang zijn.
3. Bij de communicatie tussen een service provider (Cluster 3) en een cloud provider (Cluster 2) kan er metadata ontstaan, die het mogelijk maakt een voertuig te volgen, denk bijvoorbeeld aan een implementatie waarbij een ID als een IP-adres of de telefoon-ID van de app-gebruiker wordt gebruikt.
4. Het compliance management bij de service providers (Cluster 3) kan onvoldoende zijn om duurzame compliance te waarborgen (aanbeveling uit de vorige versie van de ketenbrede PIA).

Scope en onderzoeksvragen

De scope van deze DPIA is de Talking Traffic keten. Die keten begint bij de communicatie tussen service providers (Cluster 3) en cloud providers (Cluster 2). De interne werking van de service providers (Cluster 3) zijn formeel buiten scope van deze DPIA. Toch zijn er een aantal redenen om bij het onderzoek te kijken naar de interne werking van de service providers (Cluster 3):

- Het genereren van de ID's en de route segments vindt bij de service providers (Cluster 3) plaats, vaak al binnen de app zelf.
- In de publieke opinie kunnen privacy problemen binnen service providers (Cluster 3) uitstralen op de hele keten.
- Een duurzame mitigatie van privacy problemen is afhankelijk van duurzaam compliance management. Standaarden en implementaties veranderen en de omgeving kan veranderen. Daardoor kunnen er nieuwe problemen ontstaan rond privacy. Compliance management waarborgt het proces van monitoren van de privacy en het, indien nodig, nemen van maatregelen.

Daarom zijn in dit onderzoek de volgende onderzoeksvragen richting de service providers (Cluster 3) gesteld:

1. Wat is de architectuur van het systeem, hoe lopen de datastromen?
2. Wat is het datamodel van die interne datastromen?
3. Hoe zijn de ID's die gebruikt worden gegenereerd?
4. Hoe zijn de route-segments samengesteld?
5. Welk onderdeel voert de communicatie met de cloud provider (Cluster 2) uit? Is daar een potentie voor een lek van metadata?
6. Is er documentatie beschikbaar over de opvolging van aanbeveling 5 uit de vorige DPIA: doorlopend compliance management?

De onderzoekers hebben van alle leveranciers documentatie ontvangen over deze punten, in een aantal gevallen zijn aanvullende vragen gesteld. De interne werking van de systemen van de service providers zijn zowel vanuit commercieel opzicht als vanuit security management vertrouwelijk. Daarom geeft deze rapportage de conclusies over deze punten weer, maar zijn details over de interne werking niet weergegeven. Het doel van dit deel van het onderzoek is om de interactie tussen service providers en cloud providers en iVRI leveranciers beter te begrijpen, niet om de individuele leveranciers te beoordelen. Daarom zijn in de weergave de namen van de leveranciers weggelaten.

Aanbieder A

Aanbieder A levert apps voor zowel prioriteitgerechtigd verkeer als niet-prioriteitgerechtigd verkeer. Deze apps communiceren allemaal met dezelfde backend. De backend integreert de service provider (Cluster 3) en de cloud provider (Cluster 2) functionaliteit. De apps loggen in op de backend met een robuust gegenereerd pseudoniem en sturen een constantie locatiestroom naar de backend. Vanuit de iVRI's (Cluster 1) ontvangt de backend onder andere MAP, SPAT en SSM berichten. Pas in de interface met UDAP worden de CAM berichten zoals de ETSI-standaard die voorschrijft, gegenereerd. De CAM berichten krijgen per kruispunt een eigen random gegenereerde ID. De CAM berichten bevatten geen route segments maar losse locaties. De backend vormt een barrière tegen het lekken van metadata. Aanbieder A is ISO-27001 gecertificeerd.

Aanbieder B

Aanbieder B levert de backend voor twee apps, die beiden worden gebruikt in voertuigen die prioriteitsgerechtigd kunnen zijn. Een van de apps moet met een account authenticeren op de backend de andere gebruikt een random gegenereerde maar stabiele device ID. De apps ontvangen SSM berichten terug. De apps geven aan de backend locaties door en, indien

beschikbaar, route segmenten met de verwachte route. De backend heeft een interface voor de communicatie met cloud providers (Cluster 2). De uitgaande CAM berichten hebben een ID per kruispunt. Dit ID is voorspelbaar. De backend vormt een barrière tegen het lekken van metadata. Aanbieder B heeft een geïntegreerd kwaliteitsmanagement en security management systeem. In dit management systeem neemt Aanbieder B ook controls op naar aanleiding van eerdere bevindingen. Aanbieder B is onder andere ISO-27001 gecertificeerd.

Aanbieder C

Aanbieder C levert apps voor zowel prioriteitsgerechtigd verkeer als voor niet-prioriteitsgerechtigd verkeer. Daarnaast is Aanbieder C ook cloud provider (Cluster 2). De communicatie tussen service provider (Cluster 3) en cloud provider (Cluster 2) verloopt via een proprietary interface. Deze interface stuurt, naast de message ID's, bij SRM berichten ook een UserID mee. Bij de datastromen tussen service provider (Cluster 3) en cloud provider (Cluster 2), is de ID van de berichten stabiel gedurende een sessie. Bij de route segmenten laat service provider (Cluster 3) het begin en het eind van de rit weg, maar geeft het wel de rest van de route consequent door. Bij de communicatie van cloud provider (Cluster 2) naar UDAP genereert cloud provider (Cluster 2) losse CAM berichten met een beperking van de route segmenten tot het gebied van een specifieke iVRI en een unieke ID voor de CAM berichten voor die iVRI. De prioriteitsaanvragen (SRM berichten) worden door de hele keten bevestigd met SSM berichten. Zowel service provider (Cluster 3) als cloud provider (Cluster 2) genereert ID's, dit doen ze op robuuste wijze met standaard libraries. De architectuur van service provider (Cluster 3) vormt een barrière tegen het lekken van metadata. Het security management is ISO-27001 gecertificeerd en legal department is actief betrokken.

Aanbieder D

Aanbieder D heeft twee apps die beiden worden gebruikt in voertuigen die prioriteitsgerechtigd kunnen zijn. De apps hebben elk een eigen backend die op hun beurt weer communiceren met een backend die de cloud provider (Cluster 2) interface vormt. Die interface ontvangt SSM berichten terug. De berichten vanuit de app bevatten een ID die per gebruikssessie van de app random gegenereerd wordt en route updates versturen die zowel route historie als de verwachte route bevatten. De cloud provider (Cluster 2) genereert per kruispunt een ID die bestaat uit een leverancierscode + een random deel en verstuurt de positie, snelheid en richting van de weggebruiker. De service provider (Cluster 3) interface vormt een barrière tegen het lekken van metadata. Aanbieder D is ISO-27001 gecertificeerd. De verklaring van toepasselijkheid van de ISO-27001 certificering heeft een relevante uitsluiting: de beveiliging van de verbindingen van de eigen software.