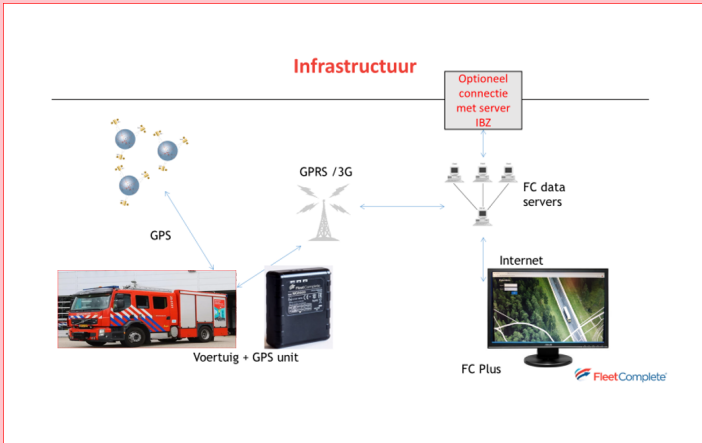


Model Data Privacy Impact Assessment

1.1 Gegevens betreffende het proces

Vul informatie betrekking hebbende op het proces, het beleid of de activiteit (er zal alleen naar 'het proces' verwezen worden, ongeacht waarvoor de DPIA wordt uitgevoerd) hieronder in, en geef toelichting waar nodig:

1	Naam van het proces	Rittenregistratie
2	Naam van de functioneel verantwoordelijke(n)	Jeroen Faber (Wagenparkbeheerder Veiligheidsregio Utrecht).
3	Beschrijving van het proces, met specificatie van de verwerking van persoonsgegevens	Registratie van datum, tijd, beweging en verkeersparameters van uitruk- en dienstvoertuigen bij de Brandweer. De voertuigen worden alleen zakelijk gebruikt. Deze DPIA beschrijft: - Proces 1: Opslag en doorgifte van mogelijke (persoons-)gegevens door een in een voertuig ingebouwd ritregistratiesysteem. - Proces 2: Registratie van mogelijke (persoons-)gegevens in een centraal bereikbare applicatie die door een verwerker aangeboden wordt door middel van hosting.  Via het ritregistratiesysteem dat ingebouwd is in een voertuig is worden allerlei gegevens verzameld en doorgegeven aan een centrale applicatie. Via een simkaart die zich in het systeem bevindt worden deze gegevens doorgegeven aan de centrale applicatie. Deze gegevens zijn echter nog geen persoonsgegevens. Het ritregistratiesysteem “weet” niet wie er op dat moment achter het stuur zit. Toch is er sprake van herleidbare gegevens tot een natuurlijke persoon, onder andere doordat een voertuig vooraf gereserveerd dient te worden. De persoon op wiens naam een voertuig is gereserveerd is in het bezit van een unieke elektronische sleutel, een zogenaamde tag. Met behulp van deze tag is het mogelijk om een voertuig te starten. Daardoor is het eenvoudig om een link te leggen tussen voertuig en bestuurder. Resumerend: De voornaam en achternaam van de bestuurder kunnen achterhaald worden door de voertuig- en ritgegevens van datum en tijd te combineren met de unieke identificatie en gegevens van een taghouder. Het gaat dus om gewone persoonsgegevens als “naam” en “achternaam” van de bestuurder van het voertuig alsmede “locatie” en niet om bijzondere persoonsgegevens.

4	Opsomming van alle persoonsgegevens die mogelijk verwerkt zullen worden, en voor welk doel	Tagnummer wordt gekoppeld aan een bij een persoon. Bij de VRU gebeurt de koppeling van persoonsgegevens met de tag in de applicatie Rittenregistratie door de Servicedesk I&I. De Servicedesk I&I ziet in de applicatie de VRU-sleutel en de voornaam en achternaam medewerker. Het doel is te weten welke medewerker welke tag heeft. Verder wordt de dag waarop er gereden is bijgehouden, de afgelegde afstand, de snelheid, de route (incl. locatie) etc.
5	Definieer de 'verantwoordelijke'	Verwerkingsverantwoordelijke: Algemeen Bestuur van de Veiligheidsregio Utrecht.
6	Beschrijving van eventuele bijzondere categorieën persoonsgegevens	N.v.t.
7	Beschrijving van hoe de persoonsgegevens verwerkt zullen worden	Een ritregistratiesysteem bestaat uit hard- en software die wordt ingebouwd in een voertuig. Vanuit het systeem dat zich in de voertuigen bevindt wordt met behulp van mobiele data een versleutelde verbinding opgezet met een centrale applicatie van de verwerker, de leverancier van de applicatie. In deze applicatie worden de ontvangen gegevens opgeslagen en beheerd. Deze zijn benaderbaar door de VRU door middel van een afgewogen authenticatie- en autorisatiemodel beschermd door een informatiebeveiligingsbeleid dat gebaseerd is op ISO 27001. De gegevens worden gebruikt voor overzichten ter ondersteuning van voldoen aan fiscale eisen, voor te nemen acties bij storingen en meldingen en dagelijks beheer om te zien of er geen grote afwijkingen plaatsvinden.
8	Beschrijving van hoe de betrokkenen geïnformeerd worden	Bij ontvangst van de tag tekent de medewerker het document 'Verklaring gebruik dienstauto' met de verklaring "zich bewust te zijn van de gegevens die geregistreerd worden bij het gebruik van een dienstoperaatort van de VRU".
9	Beschrijving van hoe gegevens actueel en correct gehouden worden	Bij indienst worden tags uitgegeven en bij uitdienst worden tags ingenomen door de leidinggevende of de Servicedesk. De tag wordt op de persoon uitgegeven en de persoon houdt de tag bij zich. Tags worden niet uitgewisseld of geruild.
10	Beschrijving van de categorieën betrokkenen (bijv. werknemers, burgers, etc.)	Werknemers (ambtenaren en vrijwilligers) en ZZP-ers.
11	Beschrijving van eventuele derde partijen (buiten de VRU) met wie de persoonsgegevens gedeeld zouden kunnen worden, en of er met zulke partijen een 'verwerkersovereenkomst' is	Leverancier: Op de kastjes in de auto worden versleutelde gegevens bewaard. (zie PvE eis 5.2-36).
12	Gaan er persoonsgegevens de grens over? (bijv. worden deze in het buitenland opgeslagen)	Registratie en doorgifte van het rittenregistratiesysteem vindt plaats binnen de EER (Europese Economische Ruimte). De persoonlijke gegevens worden in de applicatie bewaard.
13	Beschrijving van hoe en waar de persoonsgegevens worden opgeslagen	Tagnummer staat in applicatie Rittenregistratie. De persoonlijke gegevens (voornaam en achternaam) worden in de applicatie bewaard.
14	Beschrijving en motivatie van de bewaartermijn en het	De aangeboden oplossing garandeert dat vernietiging conform de regelgeving en aanvullende voorschriften m.b.t. bewaren en vernietigen van

	proces om na aflopen daarvan persoonsgegevens te verwijderen	de Archiefwet 1995 uitgevoerd kan worden: bestanden zijn pas vernietigd als zij op geen enkele wijze meer terug te halen c.q. te reconstrueren zijn.
15	Beschrijving en motivatie van de rechtsgrond voor de verwerking	De rechtsgronden voor bijhouden van de gegevens per tag zijn: ▪ Het adequaat kunnen voldoen aan fiscale regelgeving * ▪ Het halen van duurzaamheidsambities zoals de co2 prestatieladder ▪ Feiten verzamelen in geval van een aanrijding of ongeval (snelheid, wel/geen signalen, wel/niet geremd). ▪ Het evalueren van rijgedrag, evaluatie van en voldoen aan de brancherichtlijn Optische en Geluidssignalen en het kunnen toewijzen van bekeuringen. *= Op een administratieve registratie voor de belastingdienst en accountant is wel een verplichte bewaartermijn van 7 jaar van toepassing, maar deze kan in principe ook, op echter niet-efficiënte wijze, mogelijk bereikt worden zonder inzet van ritregistratiesystemen. Daarom wordt inzet van een ritregistratiesysteem ook voor dat doel als proportionele maatregel beschouwd.
16	Beschrijving van het risico van onrechtmatig gebruik en/of verlies van de persoonsgegevens, de gevolgen voor de betrokkene, en de kans op zo'n gebeurtenis	De medewerker moet zijn tag goed bewaren en niet afgeven aan een andere persoon. De kans hierop is klein. Medewerkers zijn gewend aan persoonlijke sleutels en tags. De applicatie is beveiligd via SSO en met een autorisatiematrix.
17	Beschrijving van proces waarmee betrokkenen hun rechten kunnen laten uitvoeren (bijv. rectificatie, verwijdering, beperking van verwerking, bezwaar maken tegen verwerking)	De Wagenparkbeheerder kan de rit aanpassen. Bij de rit staat 'gewijzigd'. Er is geen logging van de wijzigingen. Wanneer komt dit voor? De wagenparkbeheerder wijzigt een rit als er een boete wordt uitgekeerd en de taghouder geeft aan de tag is uitgeleend aan een andere werknemer.
18	Beschrijving van technische en organisatorische maatregelen	Beschrijf de maatregelen om de beschikbaarheid, integriteit, vertrouwelijkheid (BIV) te garanderen. -- Met behulp van een zogenaamde dongel of black box (een apparaat, data verzamelaar, die in het voertuig kan worden geplaatst) wordt verzamelde data doorgestuurd naar de cloud. Er is sprake van versleutelde opslag van gegevens. Elke dongel heeft een unieke 'encrypted security key', hetgeen betekent dat elke dongel of black box een aparte eigen versleuteling heeft. Vervolgens worden de verzamelde data uit de dongel gehaald en versleuteld geplaatst op een server van Amazon Ierland. Aldaar wordt de data ontsleuteld en vindt er 'route matching' (het koppelen van de weg locatie) plaats. Hierbij is sprake van verwerking van grote hoeveelheid data. Daarvoor gebruikt <naam applicatie> kaarten leverancier Here Maps. <naam applicatie> ontvangt ruwe gps punten welke door het programma van Here Maps worden verwerkt tot een exacte locatie op de kaart. Here Maps is een (sub)verwerker van naam applicatie. Met Here Maps heeft naam applicatie een verwerkersovereenkomst gesloten. Verrijking van de ontvangen gegevens vindt plaats op rijgedrag analyse. De snelheid, acceleratie, remmen en periode stationair draaien van de rit wordt omgevormd tot een rijscore. Nadat de gegevens zijn verrijkt worden de data op de servers opgeslagen. De persoonsgegevens en de ritgegevens (o.a. locatie gegevens) worden op twee verschillende servers opgeslagen. Hierdoor wordt het nagenoeg

		onmogelijk gemaakt om de locatiegegevens aan een persoon te koppelen. Van beide servers wordt een backup gemaakt op twee backup servers. De gegevens worden op de servers versleuteld opgeslagen. Door gebruikmaking van een webapplicatie kan de werkgever de aangegeven gegevens inzien. Aan de werkgever wordt de mogelijkheid geboden de berijder inzicht te geven in zijn data via een app.
19	Overige informatie	N.v.t.

1.2 Beoordeling van wetmatigheid van het proces

1	Beoordeling van doelbepaling en legitimiteit van verwerking, en motivatie	Doelmatigheid van de verwerking van de volgende gegevens: Ritregistratie-> alleen zakelijke kilometers want je kan met de auto alleen zakelijk rijden. Brandstofgebruik -> tanklocatie is noodzakelijk ter voorkoming van fraude. Parkeerbeheer -> parkeerzone, kenteken en duur is noodzakelijk voor belasting. Rijgedrag -> voor snelheidsovertredingen en analyses voor ongevallen Live track & trace -> locatie kan noodzakelijk zijn voor de bedrijfsvoering.
2	Beoordeling van algemene technische en organisatorische maatregelen, en motivatie	?
3	Beoordeling van noodzaak en motivatie	
4	Beoordeling van rechten van betrokkenen en motivatie	?
5	Aanvullende eisen voor goedkeuring (indien nodig)	
6	Overige	

1.3 Risico-inventarisatie en -beoordeling

Nr	Beschrijving risico	Kans	Impact	Beheersmaatregelen & verantwoordelijken
1.	De specifieke regels voor bewaartermijnen worden mogelijk niet toegepast.	Laag	Hoog	Automatisering in de software van de verwerker.
2.	Systeem kan gebruikt worden als personeelsvolgsysteem	Hoog	Midden	Autorisatiematrix in de centraal aangeboden applicatie met rollen die gebaseerd zijn op afgewogen functieprofielen. Leg deze autorisatiematrix duidelijk vast in het applicatieregister in overleg met de CISO van de beide veiligheidsrisico's.
3.	Gebruik van het systeem buiten de kaders waarvoor het bedoeld is	Laag	Hoog	Medewerkers leggen ambtseed of –belofte af en houden zich aan ambtenarenwet en de principes die daarin verwoord zijn.
4.	Doeleinden van black boxes zijn niet voldoende bekend bij medewerkers	Midden	Laag	Medewerkers bij indiensttreding laten tekenen voor tag dienstvoertuigreglement. Zittend personeel wordt persoonlijk geïnformeerd en gevraagd te

				tekenen voor akkoord. Voor Veiligheidsregio's Flevoland en Veiligheidsregio Gooi en Vechtstreek: stel een specifieke tekst samen die kan worden toegevoegd aan de formele privacyverklaringen op de websites van de Veiligheidsregio's
5.	Persoonsgegevens in rapportage	Laag	Hoog	Leverancier dient uitsluitend geanonimiseerde rapportages vanuit de applicatie te genereren die bovendien voldoen aan het principe van dataminimalisatie. In rapportage dient er rekening mee gehouden te worden dat een gepseudonimiseerd identificatienummer mogelijk te herleiden is tot een natuurlijke persoon. Een gepseudonimiseerd (persoons)gegeven wordt nog steeds beschouwd als een persoonsgegeven en valt onder de AVG. Neem daarom ook geen gepseudonimiseerde (persoons)gegevens op in een rapportage.
6.	Medewerker wordt onterecht aangesproken op rijgedrag met consequenties voor bijvoorbeeld rechtspositie.	Midden	Laag	Persoonsgegevens worden alleen in opdracht van de direct leidinggevende verstrekt. In geval van een mogelijk strafrechtelijk onderzoek of vragen vanuit politie/justitie alleen via hoogst leidinggevende
7.	Er is geen proces ingericht voor het verwijderen van persoonsgegevens, het is onduidelijk of logbestanden en/of back-ups verwijderd kunnen worden en het beleid omtrent de verwijdering van de logbestanden ontbreekt.	Hoog	Laag	Verwijder persoonsgegevens, logbestanden en back-ups tijdig. Opdracht geven aan verwerker c.q. leverancier om dit te organiseren. Leg dit vast in de verwerkersovereenkomst met de verwerker c.q. leverancier.
8.	Ontbreken technische en organisatorische beveiligingsmaatregelen	Hoog	Hoog	Adviesmaatregel: De beide veiligheidsregio's hebben een informatiebeveiligingsbeleid dat zal voldoen of voldoet aan de toepasselijke norm, de ISO 27001 en/of de BIO. Zorg ervoor dat de juiste technische en organisatorische beveiligingsmaatregelen zijn opgenomen in een verwerkersovereenkomst met de leverancier c.q. verwerker. Neem daarin op dat de verwerker ISO 27001 gecertificeerd is en voldoet aan de branchestandaard voor ritregistratiesystemen die een sluitende rittenadministratie oplevert

				voor fiscale toepassingen, het Keurmerk Ritregistratiesystemen dat ook een gedragscode heeft opgesteld. Deze gedragscode is mede samengesteld door de Branchevereniging Leveranciers Ritregistratiesystemen (BVLRL) en Vereniging Zakelijke Rijders (VZR). De Verwerker dient op eigen kosten en lasten passende technische en organisatorische maatregelen te nemen en te handhaven met betrekking tot de Verwerking en beveiliging van Persoonsgegevens en in het bijzonder in overeenstemming met de artikelen 32-34 van de AVG, waaronder onder meer en waar van toepassing: • Het vermogen om de doorlopende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te waarborgen; • Het vermogen om de beschikbaarheid en toegang tot Persoonsgegevens tijdig te herstellen in geval van een fysiek of technisch incident; • Een procedure voor het regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de beveiliging van de Verwerking te waarborgen. • De Verwerker zorgt ervoor dat dergelijke technische en organisatorische maatregelen geschikt zijn voor de specifieke risico's die bij haar verwerkingsactiviteiten aanwezig zijn, in het bijzonder om persoonsgegevens te beschermen tegen de onopzettelijke of onwettige vernietiging, verlies, wijziging, ongeautoriseerde openbaarmaking ervan of toegang ertoe. • De verwerker implementeert en onderhoudt op eigen kosten en lasten de technische en organisatorische maatregelen.
9.	Loggegevens zijn inzichtelijk voor onbevoegden (Wie heeft wanneer naar welke gegevens gekeken?)	Midden	Hoog	Neem een specifieke rol op voor deze functionaliteit in de autorisatiematrix van de applicatie en ga zorgvuldig om met de toekenning ervan.

--	--	--	--	--

Kans en impact: laag/middel/hoog

Richtlijn voor beoordeling:

- *Kans – laag: vrijwel nooit, of minder vaak dan eens elke paar jaar*
- *Kans – middel: ongeveer eens per jaar*
- *Kans – hoog: vaker dan eens per jaar*
- *Risico – laag: er is geen, of slechts een verwaarloosbaar risico voor de betrokkene. Er zijn geen bijzondere categorieën persoonsgegevens betrokken.*
- *Risico – middel: er is een risico voor de privacy van de betrokkene, maar de betrokkene ondervindt geen fysieke, sociale of financiële schade. Risico is altijd middel of hoog als er bijzondere categorieën persoonsgegevens betrokken zijn, ongeacht wat voor schade mogelijk is.*
- *Risico – hoog: er is een risico voor fysieke, sociale of financiële schade voor de betrokkene. Risico is altijd middel of hoog als er bijzondere categorieën persoonsgegevens betrokken zijn, ongeacht wat voor schade mogelijk is.*

1.4 Restriscio

Aan de hand van de risico-inventarisatie en -beoordeling in 1.3 blijven enkele restriscio's over. Hieronder wordt beoordeeld of deze aanvaardbaar zijn:

Nummer	Beschrijving restriscio	Beoordeling
1.	?	
2.		

1.5 Vaststelling DPIA

De functionaris voor de gegevensbescherming bevestigt hierbij dat de voorgestelde verwerking aanvaardbaar is

Naam:

Datum:

Opmerkingen:

Handtekening:

De DPIA wordt vastgesteld door een directeur:

Naam:

Datum:

Handtekening: