Data protection impact assessment (DPIA) Ritregistratiesystemen uitruk- en dienstvoertuigen

Door
Veiligheidsregio Flevoland en Veiligheidsregio Gooi en Vechtstreek

Inhoudsopgave

Inleiding

In uitruk- en dienstvoertuigen van de brandweer van de Veiligheidsregio's Flevoland en Gooi en Vechtstreek wordt door beide veiligheidsregio's gebruik gemaakt van ritregistratiesystemen, of zal in de nabije toekomst gebruik worden gemaakt van ritregistratiesystemen.

De wijze waarop wordt omgegaan met "tot natuurlijke personen herleidbare gegevens" die gedurende ritten of na opslag van gegevens uit deze systemen beschikbaar zijn valt onder de Algemene verordening gegevensbescherming (AVG).

Deze Data Protection Impact Assessment (DPIA) ofwel gegevensbeschermingseffectbeoordeling is opgesteld om te verduidelijken op welke wijze de beide veiligheidsregio's invulling geven aan een zorgvuldige en verantwoordelijke verwerking van persoonsgegevens die door deze ritregistratiesystemen in voertuigen van de Veiligheidsregio's Flevoland en Gooi en Vechtstreek vastgelegd worden. De gegevens worden ook doorgegeven worden aan een applicatie ter registratie. In deze DPIA wordt een afweging gemaakt tussen de noodzaak van verwerking enerzijds ten opzichte van een mogelijk risico voor de rechten en vrijheden van natuurlijke personen, doordat verwerking van deze gegevens herleidbaarheid tot personen tot gevolg kan hebben.

Deze DPIA richt zich onder andere op:

- De verwerking van persoonsgegevens in het kader van de ritregistratiesystemen in voertuigen en de rechtmatigheid hiervan.
- De genomen of te nemen passende organisatorische en technische maatregelen daar waar de persoonsgegevens voorkomen en de beoordeling hierop.
- Eisen van privacy by design van het technisch ontwerp van dataopslag en de toets op deze thema's.

Door uitvoeren van deze DPIA wordt, voor zover van toepassing, voldaan aan een verplichting die opgelegd is in het "Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens" zoals gepubliceerd in de Staatscourant 64418 van 27 november 2019.
Hierbij wordt aangetekend door de Veiligheidsregio's Flevoland en Gooi en Vechtstreek dat deze lijst van verwerkingen van persoonsgegevens niet uitputtend is en dat het kan zijn dat een verwerking van persoonsgegevens niet op de lijst in het besluit staat, maar, gelet op de aard, de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen en aldus een gegevensbeschermingseffectbeoordeling (DPIA) moet worden gedaan.

Ritregistratiesystemen kunnen zich bijvoorbeeld bevinden in de volgende uitruk- en dienstvoertuigen bij de brandweer van de beide veiligheidsregio's:

- Tankautospuiten
- Redvoertuigen
- Piketvoertuigen
- Op naam te reserveren dienstvoertuigen
- Etc.

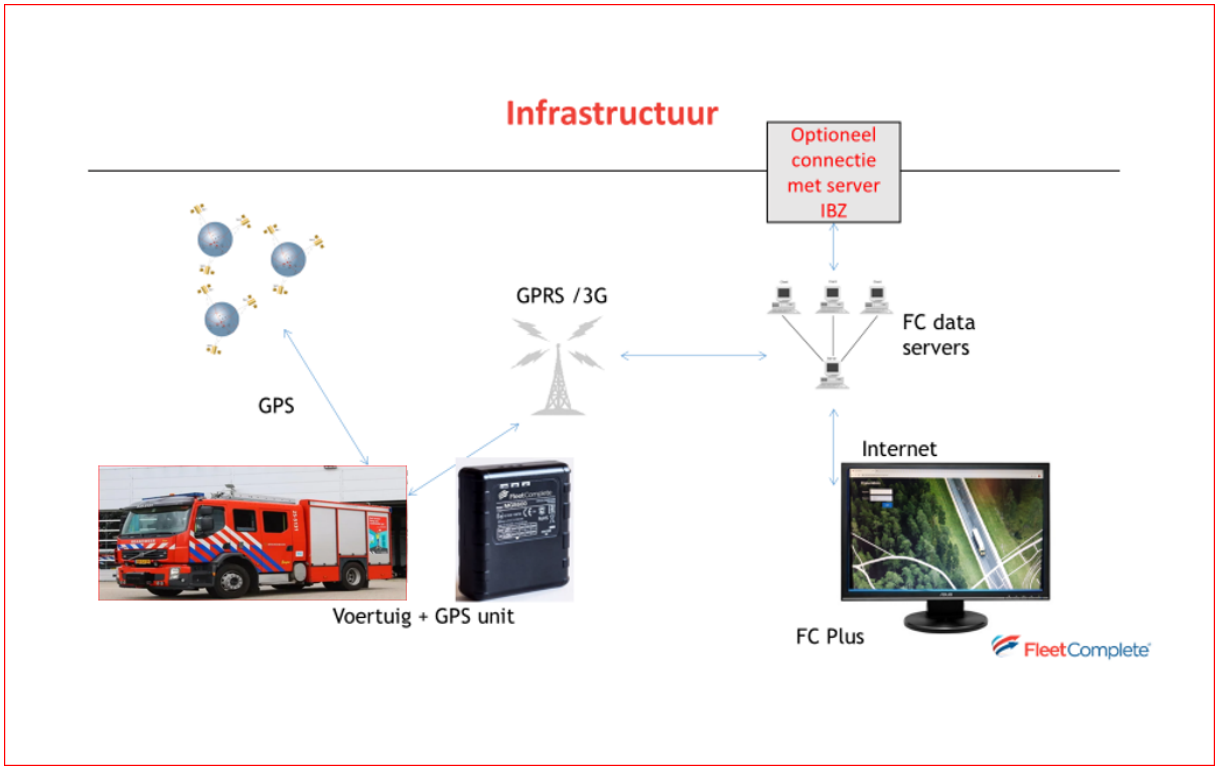
1. Beschrijving proces

Registratie van datum, tijd, beweging en verkeersparameters van uitruk- en dienstvoertuigen bij de Brandweer.

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.

Genoemde processen zijn weergegeven in onderstaande afbeelding.



2. Persoonsgegevens

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.

Het ritregistratiesysteem houdt onder andere exact bij wanneer een specifiek voertuig gereden heeft. Daardoor is het eenvoudig om een link te leggen tussen voertuig en bestuurder. Zonder de combinatie met informatie over de taghouder, de gebruiker van een unieke elektronische sleutel, zijn de gegevens die tijdens de rit vastgelegd worden nog niet herleidbaar tot een natuurlijke persoon.

Resumerend: Door middel van raadpleging van de centrale applicatie kunnen voornaam en achternaam van de bestuurder 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.

3. Gegevensverwerking

Het ritregistratiesysteem verwerkt de volgende gegevens:

- Tijdstip
- Datum rit
- Locatie
- Ritgegevens
- Gedrag (niet voldoen aan afspraken en regels) en rijstijl.

4. Verwerkingsdoeleinden

De doeleinden van de verwerking van de gegevens door de ritregistratiesystemen zijn:

- Het voldoen aan regels omtrent belasting.
- Het monitoren van duurzaamheidsmetrics.
- Onderhoud en beheer van het wagenpark.
- Feiten verzamelen in geval van een aanrijding of ongeval (snelheid, wel/geen signalen, wel/niet geremd).
- Evaluatie rijgedrag en toewijzen bekeuringen.

5. Betrokken partijen

Verwerkingsverantwoordelijke: Veiligheidsregio's Flevoland en Gooi en Vechtstreek zijn de verwerkingsverantwoordelijken voor een verwerking van persoonsgegevens door of via ritregistraties, zoals hierin voorgesteld.

Verwerker: De partij die in opdracht van Veiligheidsregio's Flevoland en Gooi en Vechtstreek de centrale applicatie waarin de registratie plaatsvindt, host en beheert (n.t.b.)

6. Belangen bij gegevensverwerking

De belangen van de VRGV en de VRF zijn:

- Voldoen aan regelgeving omtrent belasting,
- Zorgplicht medewerkers in geval van ongevallen,
- het verbeteren van de duurzaamheid van het wagenpark,
- Verantwoording aan accountant,
- T&L i.v.m. preventief en correctief onderhoud, verantwoording wagenpark,
- Facilitair vim reserveringen en schadeafhandeling verzekeraar,
- Kostenaspect wagenpark, inzetbaarheid personeel en in stand houden imago.

7. Verwerkingslocaties

Registratie en doorgifte vindt plaats binnen de EER (Europese Economische Ruimte). De gegevensopslag vindt plaats op een server die binnen de grenzen van de EER is opgesteld.

8. Techniek en methode van gegevensverwerking

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 Veiligheidsregio's Flevoland en Gooi en Vechtstreek door middel van een afgewogen authenticatie- en autorisatiemodel beschermd door een informatiebeveiligingsbeleid dat gebaseerd is op ISO 27001.

9. Juridisch en beleidsmatig kader

Algemeen:

De Veiligheidsregio's Flevoland en Gooi en Vechtstreek voeren een taak van algemeen belang of van openbaar gezag uit dat aan de verantwoordelijke is opgedragen (art. 6 lid 1 sub e, AVG). De Wet veiligheidsregio's beschrijft deze taken. In het kader van de wettelijke taken wordt gebruik gemaakt van voertuigen die eigendom zijn van de veiligheidsregio's. Omdat aan het gebruik van deze voertuigen door ambtenaren en vrijwilligers mogelijk invloed heeft op de (mate waarin) belasting betaald moet worden, dient er bijgehouden te worden welke persoon op welk moment in het voertuig rijdt. Daarbij kunnen verkeersboetes ook aan individuele personen worden doorberekend, als deze onwettig zijn veroorzaakt (bijvoorbeeld tijdens het rijden in voertuigen met optische- en geluidssignalen, zonder dat de vrijstelling van kracht was). Ten slotte hebben de veiligheidsregio's de verplichting om te proberen de 'carbon footprint' te verkleinen waar mogelijk. De gegevens die beslissingen ten aanzien van deze plicht voeden komen onder andere uit het ritregistratiesysteem.

10. Bewaartermijn

Daar waar mogelijk persoonsgegevens worden opgeslagen (zoals in de centraal aangeboden applicatie door de verwerker) geldt een maximale bewaartermijn van 7 jaar. Dit heeft te maken met de verplichte bewaartermijn door fiscale wet- en regelgeving zoals vastgelegd in Artikel 52 van de Algemene Wet Inzake Rijksbelastingen (AWR).

B. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

In de zin van de AVG is de grondslag voor verwerking van persoonsgegevens voor alle aangegeven doeleinden een “wettelijke verplichting” (art. 6 lid 1 sub c, AVG).

12. Rechtsgrond (Bijzondere) persoonsgegevens

Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Verwerking van bijzondere categorieën van persoonsgegevens door het ritregistratiesysteem of in een centraal aangeboden applicatie is niet aan de orde. Deze categorie van gegevens wordt niet verwerkt.

13. Doelbinding

De persoonsgegevens die mogelijk worden verzameld en verwerkt worden uitsluitend gebruikt voor de doeleinden:

1. Het voldoen aan regels omtrent belasting.
2. Het monitoren van duurzaamheidsmetrics.
3. Onderhoud en beheer van het wagenpark
4. Feiten verzamelen in geval van een aanrijding of ongeval (snelheid, wel/geen signalen, wel/niet geremd).
5. Evaluatie rijgedrag en toewijzen bekeuringen

14. Noodzaak en evenredigheid

De AVG verplicht dat persoonsgegevens enkel worden verwerkt wanneer ze noodzakelijk zijn voor het bereiken van het doel van de verwerking. Dit wil zeggen dat er niet te veel persoonsgegevens moeten worden verwerkt voor het te bereiken doel (dataminimalisatie).

Voor de set van persoonsgegevens die eerder gespecificeerd is in hoofdstuk 2 is aannemelijk dat het genoemde doel niet te bereiken is zonder de verwerking van deze persoonsgegevens.

Op basis van de in deze DPIA beschreven processen worden geen persoonsgegevens verwerkt waarbij sprake is van een onevenredige inbreuk op de persoonlijke levenssfeer. Er worden geen bijzondere persoonsgegevens verwerkt.

De noodzaak wordt hieronder per doel nog eens kort beschreven:

- Het adequaat kunnen voldoen aan fiscale regelgeving
- Het halen van duurzaamheidsambities zoals de co2 prestatieladder
- Onderhoud en beheer van het wagenpark en daarmee kunnen voldoen aan veiligheids- en kwaliteitsnormen
- 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.

15. Rechten van betrokkenen

Het is de taak van de organisatie om de betrokkene te informeren over zijn of haar rechten, alsmede aan te geven tot wie de betrokkene zich kan wenden in kader van zijn of haar rechten.

In de privacyverklaringen van de Veiligheidsregio's Flevoland en Gooi en Vechtstreek die op de websites van de organisaties te vinden zijn wordt aangegeven hoe deze rechten uitgeoefend kunnen worden. Onder meer is in de privacyverklaringen het volgende te vinden:

- Onze werkwijze
- Wanneer registreren wij persoonsgegevens?
- Jouw rechten
- Hoe kun je je gegevens inzien, wijzigen of laten wissen?
- Functionaris gegevensbescherming

16. Vertrouwelijkheid en integriteit

<u>Technische beveiligingsmaatregelen</u>

ISO 27001 en/of BIO (Baseline Informatiebeveiliging Overheid).

De volgende beveiligingsmaatregelen zijn op verzending en dataopslag van black box-gegevens genomen:

1. *Authenticatie*
   a. De authenticatie verloopt via het IDU-principe zoals dat vormgegeven is in het informatiebeveiligingsbeleid van veiligheidsregio's Flevoland en G&V.

2. *Autorisatiemanagement*
   a. Rollen & verantwoordelijkheden zijn opgenomen in autorisatiematrix.
   b. Rol gebaseerde toegang.

3. *Toegang*
   a. De toegang tot de bestanden vindt plaats via two-factor authentication.
   b. Dataopslag vindt plaats bij of via een externe partij die voldoet aan ISO 27001 en het Keurmerk Ritregistratiesystemen. Dataopslag vindt plaats binnen de EER (Europese Economische Ruimte).

4. *Versleuteling*
   a. Versleuteling wordt afgedwongen bij mogelijke uitwisseling van persoonsgegevens.

5. *Gegevensuitwisseling*
    a. Er vindt geen gegevensuitwisseling plaats met andere partijen dan verantwoordelijke en verwerker. Verwerker kan een subverwerker inschakelen.

6. *Logging & monitoring*
    a. Logging op de dataopslag.
    b. Logging op de toegang tot de logging.

7. *Back-up & herstel*
    a. Back-up sluit aan bij de huidige back-up cyclus of wordt adequaat vormgegeven bij verwerker. Back-up is beschreven in het informatiebeveiligingsbeleid van veiligheidsregio's Flevoland en G&V.

8. *Incidentmanagement*
    a. Op procesniveau, zoals vastgelegd in het informatiebeveiligingsbeleid van veiligheidsregio's Flevoland en G&V. Dit beleid is opgesteld in mei 2022.

Impactanalyse informatieveiligheid

Bovenstaande punten zijn een algemene weergave van de manier waarop onder andere de vertrouwelijkheid en de integriteit van de gegevens geborgd kunnen worden. Bij het afsluiten van nieuwe overeenkomsten of het beheren van de huidige overeenkomst is het uitvoeren van een impactanalyse met betrekking tot informatieveiligheid noodzakelijk om alle relevante zaken op dit gebied voldoende te borgen. Dit kan alleen gedaan worden in nauwe samenwerking met de Chief Information Security Officer van beide veiligheidsregio's.

17. Privacy by design en default van het technisch ontwerp

Bij de ontwikkeling van de systematiek zijn privacy (privacy by design) en informatieveiligheid toegepast op het technisch ontwerp van de applicatie(s).

18. Risico's

Hieronder is per risico kort uiteengezet wat het risico voor betrokkenen is en hoe dit risico gekwalificeerd dient te worden.
De kwalificatie wordt gemaakt op basis van kans x impact = risiconiveau. In bijlage 1 is een uitgebreide omschrijving opgenomen van de berekening en definities van kans, impact en risiconiveaus.

Risico 01: De specifieke regels voor bewaartermijnen worden mogelijk niet toegepast.

- Kans:
  De kans dat dit risico zich manifesteert is laag.
- Impact:
  De impact van dit risico zonder maatregelen is hoog aangezien de gegevens dan langer bewaard worden dan noodzakelijk is en waardoor gegevens onrechtmatig worden verwerkt.
- **Adviesmaatregel:**
  Door automatisering in de centrale software van verwerker wordt dit mechanisme geborgd.

Risico voor Betrokkene (voor maatregelen)	Laag/midden

Risico voor Betrokkene (na maatregelen)	Laag

Risico 02: Systeem kan gebruikt worden als personeelsvolgsysteem

- Kans:
  De kans dat dit risico zich manifesteert zonder maatregelen is hoog.
- Impact:
  De impact van dit risico zonder maatregelen is midden.
- **Adviesmaatregel:**
  Maak gebruik van een juiste autorisatiematrix in de centraal aangeboden applicatie(s) met rollen die gebaseerd zijn op afgewogen functieprofielen. Leg deze autorisatiematrix duidelijk vast in het applicatieregister in overleg met de CISO van de beide veiligheidsregio's.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Risico 03: Gebruik van het systeem buiten de kaders waarvoor het bedoeld is

- Kans:
  De kans dat dit risico zich manifesteert is laag.
- Impact:
  De impact van dit risico zonder maatregelen is hoog
- **Adviesmaatregel:**
  Medewerkers leggen ambtseed of –belofte af en houden zich aan ambtenarenwet en de principes die daarin verwoord zijn.

Risico voor Betrokkene (voor maatregelen)	Midden
Risico voor Betrokkene (na maatregelen)	Laag

Risico 04: Doeleinden van black boxes zijn niet voldoende bekend bij medewerkers

- Kans:
  De kans dat dit risico zich manifesteert is midden.
- Impact:
  De impact van dit risico zonder maatregelen is midden.
- **Adviesmaatregel:**
  Medewerkers bij indiensttreding laten tekenen voor druppel dienstvoertuigreglement.
  Zittend personeel wordt persoonlijk geïnformeerd en gevraagd te tekenen voor akkoord.
  Specifieke tekst samenstellen die kan worden toegevoegd aan de formele privacyverklaringen op de websites van Veiligheidsregio's Flevoland en Veiligheidsregio Gooi en Vechtstreek.

Risico voor Betrokkene (voor maatregelen)	Midden
Risico voor Betrokkene (na maatregelen)	Laag

Risico 05: Persoonsgegevens in rapportage

- Kans:
  De kans dat dit risico zich manifesteert is laag.
- Impact:
  De impact van dit risico zonder maatregelen is hoog.
- **Adviesmaatregel:**
  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.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Risico 06: Medewerker wordt onterecht aangesproken op rijgedrag met consequenties voor bijvoorbeeld rechtspositie.

- Kans:
  De kans dat dit risico zich manifesteert is midden.
- Impact:
  De impact van dit risico zonder maatregelen is hoog.
- **Adviesmaatregel:**
  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.

Risico voor Betrokkene (voor maatregelen)	Midden
Risico voor Betrokkene (na maatregelen)	Laag

Risico 07: 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.

- Kans:
  De kans dat dit risico zich manifesteert zonder maatregelen is hoog.
- Impact:
  De impact van dit risico zonder maatregelen is hoog, aangezien de gegevens langer bewaard zullen worden dan noodzakelijk is waardoor persoonsgegevens onrechtmatig zullen worden verwerkt.
- **Adviesmaatregel:**
  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.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Risico 08: Ontbreken technische en organisatorische beveiligingsmaatregelen

- Kans:
  De kans dat dit risico zich manifesteert zonder maatregelen is hoog.
- Impact:
  De impact van dit risico zonder maatregelen is 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 Brancheverenigingen Leveranciers Ritregistratiesystemen (BVLR) en Vereniging Zakelijke Rijders (VZR).

  De Verwerker dient op eigen kosten en lasten passende technische en organisat*orische 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.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Risico 09: Loggegevens zijn inzichtelijk voor onbevoegden (Wie heeft wanneer naar welke gegevens gekeken?)

- Kans:
  De kans dat dit risico zich manifesteert zonder maatregelen is midden.
- Impact:
  De impact van dit risico zonder maatregelen is hoog.
- **Adviesmaatregel:**
  Neem een specifieke rol op voor deze functionaliteit in de autorisatiematrix van de applicatie en ga zorgvuldig om met de toekenning ervan.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

Bijlage 1: Achtergrond risiconiveaus

Kans

Bij het bepalen van de kans (K) dat een risico zich voordoet worden de volgende factoren in acht genomen:

- Het bestaan van gemotiveerde en bekwame actoren met bijbehorend hun motivaties en vaardigheden;
- Aard van de kwetsbaarheid; en
- Aanwezig zijn van bestaande maatregelen en hun effectiviteit

De kans dat een potentiële kwetsbaarheid kan worden uitgebuit door een actor zal worden omgeschreven als hoog, midden, of laag. De onderstaande tabel beschrijft deze drie lagen.

Kans	Kans beschrijving
Hoog	De actor is zeer gemotiveerd en bekwaam en maatregelen ter preventie van de uitbuiting van de kwetsbaarheid zijn ineffectief.
Midden	De actor is zeer gemotiveerd en bekwaam, maar er zijn maatregelen geïmplementeerd die de uitbuiting van de kwetsbaarheid belemmeren.
Laag	De actor mist motivatie of bekwaamheid, of maatregelen zijn geïmplementeerd om de uitbuiting van de kwetsbaarheid te voorkomen of significant te belemmeren.

Impact

De impact van een geëffectueerd risico wordt beschreven in termen van verlies of beperking van beschikbaarheid, integriteit of vertrouwelijkheid van gegevens op een schaal van laag, midden en hoog. De onderstaande beschrijvingen geven een korte omschrijving van deze aspecten en de consequentie (of impact) die daaraan verbonden is als dit doel niet behaald wordt.

Verlies van integriteit – Systeem en data integriteit verwijst naar de eis dat de juistheid en volledigheid van informatie geborgd moet zijn. De integriteit is verloren als incorrecte wijzigingen zijn aangebracht in de informatie door opzettelijk of onopzettelijk handelen. Als verlies van integriteit niet (tijdig) verholpen wordt kan verder gebruik van het gecompromitteerde systeem of data resulteren in onnauwkeurigheid, fraude of beveiligingsincidenten. Verlies van integriteit kan een eerste stap zijn in een aanval op systemen met verlies van beschikbaarheid of vertrouwelijkheid tot gevolg.

Verlies van Beschikbaarheid – Als een dienst (of gegevens aangeboden door een dienst) niet beschikbaar is voor de eindgebruikers, raakt dit mogelijk de missie van de organisatie. Verlies van systeemfunctionaliteit en operationele effectiviteit kunnen leiden tot beveiligingsincidenten of verlies van productiviteit.

Verlies van Vertrouwelijkheid – Systeem en data vertrouwelijkheid verwijst naar de bescherming tegen ongeautoriseerde openbaarmaking van gegevens (o.a. verlies van bedrijfsgeheimen, intellectueel eigendom (software, protocollen, documenten, etc.), of persoonsgegevens). Ongeautoriseerde, onverwachte, of onopzettelijk openbaarmaking van persoonsgegevens kan leiden tot het schenden van wet- en regelgeving.

Impactniveau	Impactbeschrijving
Hoog	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van kritische assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene significant schaden, compromitteren of belemmeren; 3. Kan een schending van wettelijke richtlijnen veroorzaken; 4. Kan resulteren in sterfte of ernstig letsel; 5. Kan een grote inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Midden	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het kostbare verlies van materiële assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden, compromitteren of belemmeren; 3. Kan resulteren in persoonlijk letsel. 4. Kan een inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene
Laag	Misbruik van een kwetsbaarheid: 1. Kan resulteren in het verlies van bepaalde assets of middelen; 2. Kan de missie, reputatie of belang van de organisatie of Betrokkene schaden 3. Kan een kleine inbreuk opleveren in de fundamentele rechten en vrijheid van Betrokkene

Risicocalculatie

Deze stap gebruikt de kans en impact om het niveau van het risico te bepalen, op basis van de beschreven aspecten:

- De kans (K) dat een risico effectueert; en
- De impact (I) op de organisatie of Betrokkene als het risico is geëffectueerd.

Het risiconiveau wordt toegekend door een vooraf vastgestelde matrix die het belang van mitigerende maatregelen aangeeft. De combinaties van kans en impact zijn gegroepeerd in hoog (H, rood), midden (M, geel) en laag (L, groen). De matrix toont hoe de risico's zijn geclassificeerd gebaseerd op de impact en kans.

Kans / Impact	Laag	Middel	Hoog
Laag	Laag	Laag	Middel
Midden	Laag	Middel	Hoog
Hoog	Middel	Hoog	Hoog

Op basis van de risiconiveaus uit de matrix staat in de tabel hieronder beschreven welke maatregelen verwacht worden.

Risiconivo	Risico Beschrijving en te verwachten maatregel
Hoog	Als een waarneming of bevinding wordt geëvalueerd als een hoog risico, is er sterke behoefte aan corrigerende maatregelen. Een bestaand systeem kan blijven werken, maar een beveiligingsplan of andere risico-beperkende maatregel moet zo snel mogelijk worden geïmplementeerd.
Midden	Als een waarneming wordt beoordeeld als gemiddeld risico, moeten eventuele corrigerende maatregelen worden overwogen.
Laag	Als een waarneming wordt beschreven als een laag risico, kunnen corrigerende maatregelen nog steeds nodig zijn of kan het risico worden geaccepteerd.