

PRIVACYCOMPANY



Workshop DPIA iVRI's LVMB

17 april 2024

Agenda

- Introductie tot uitvoeren DPIA's
- Voorbereiding bij uitvoeren DPIA
- Beschrijving feitelijke situatie
- Beschrijving juridische verantwoording
- Beschrijving risico's
- Beschrijving maatregelen

Brief AP van 17 april 2024

<https://www.autoriteitpersoonsgegevens.nl/actueel/zorgen-ap-om-volgverkeerslichten>

De AP komt nu weer bij u op de lijn, omdat de AP onlangs bij een gemeente geconstateerd heeft dat de inzet van iVRI's allesbehalve zorgvuldig plaatsvond. Zo waren er vragen over: de noodzakelijkheid van de verwerking van persoonsgegevens; welke persoonsgegevens verzameld werden; op welke manier de persoonsgegevens verwerkt werden; door wie de gegevens precies verwerkt werden; en wie er als verwerkingsverantwoordelijke moest worden aangemerkt. Het feit dat deze vragen niet naar behoren konden beantwoord nadat hier door de AP om werd gevraagd én de AP het sterke vermoeden heeft dat dit probleem op meer plaatsen speelt dan slechts in deze ene gemeente, is zorgwekkend en reden voor de AP om u, als politiek verantwoordelijke voor de wegbeheerder Rijkswaterstaat, nogmaals te wijzen op de risico's van het gebruik van iVRI's.

Brief AP van 17 april 2024

De AP verzoekt u met klem om te bezien of de mogelijke keten van verwerkingen in het kader van iVRI's voldoet aan de regels van de AVG. Het uitvoeren van een Data Protection Impact Assessment (DPIA) kan daarbij niet alleen behulpzaam zijn, in bepaalde gevallen zal deze DPIA zelfs verplicht zijn.¹ De AP wijst er voor de volledigheid op dat een dergelijke DPIA geen eenmalige activiteit is, maar een continue exercitie. Een veranderde context, veranderende technische toepassingen of aangepaste standaarden kunnen bijvoorbeeld aanleiding zijn om een DPIA te herzien.

PRIVACYCOMPANY 

Introductie DPIA

Wat is een Data Protection Impact Assessment

Manier om privacyrisico's van een project in een vroegtijdig stadium helder en gestructureerd in beeld te brengen

Waarom een DPIA uitvoeren?

- Inzicht in het gebruik van de applicatie en/of het proces en de mogelijke risico's
- Inzicht om betere afwegingen te maken en mogelijk 'minder' ingrijpende of efficiëntere maatregelen in te zetten (ook cost-efficiency)
- Inzicht om voorbereid te zijn als er iets misgaat
- Inzicht in het afbreukrisico en kansen op boetes
- Inzicht in kans op en hoogte van materiële schade en/of reputatieschade

Waarom een DPIA uitvoeren?

Is verplicht wanneer proces/applicatie en verwerking:

- voldoet aan de criteria van artikel 35 AVG
- voorkomt op de verplichte lijst AP, o.a. nr. *'grootschalig en stelselmatig verwerken van locatiegegevens'*
- gegevens worden verwerkt in de cloud (EDPB 17 januari 2023)
- moet voldoen aan andere (verplichte) risico-analyses, zoals NIS2 en BIO

Pre-scan/DPIA

Ieder proces of applicatie onderwerpen aan een “Quickscan”

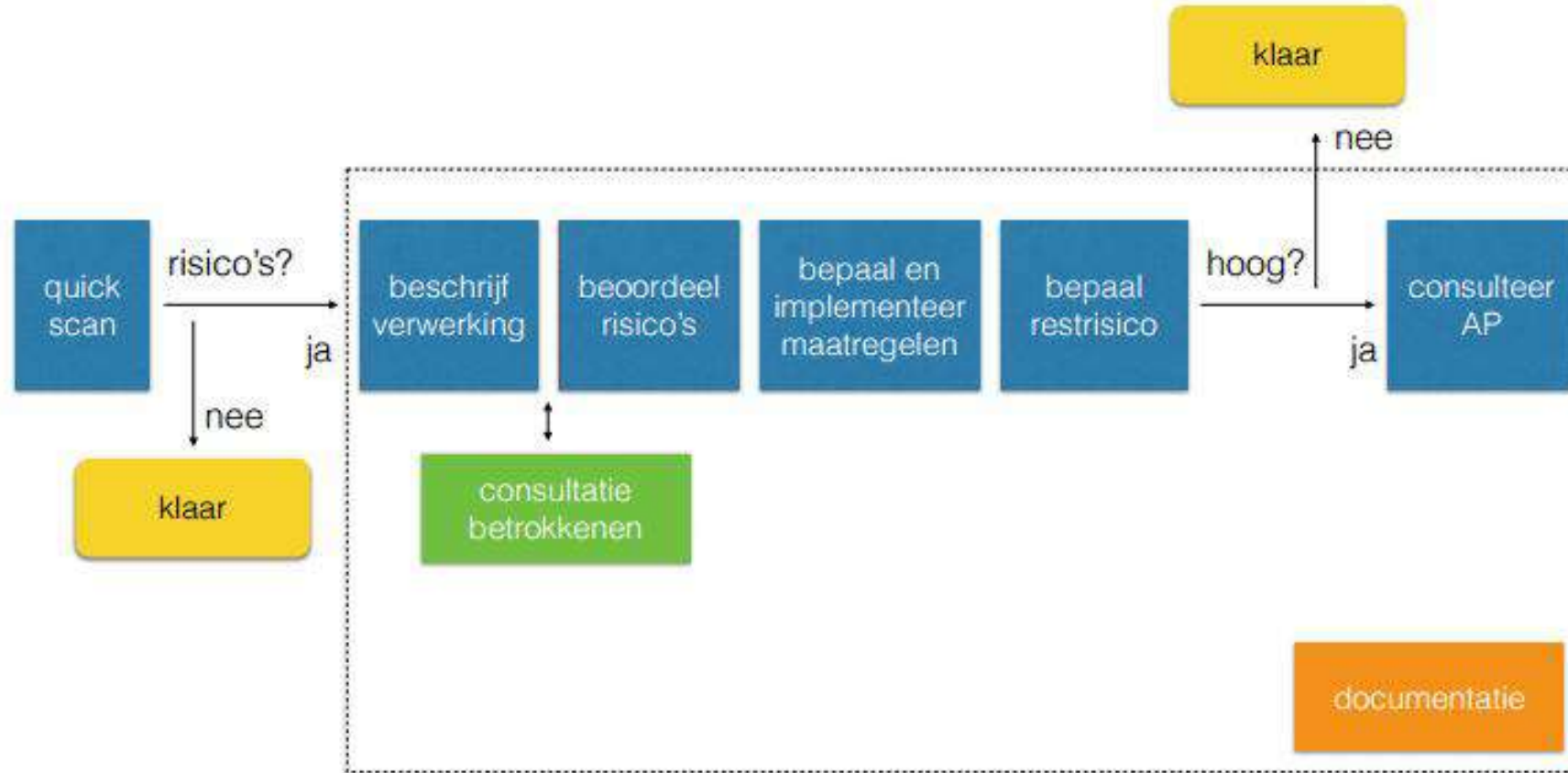
- Inzicht in wel/niet verplicht uitvoeren van een DPIA
- Borgen van uitkomsten beoordeling
- Borgen risico-inschatting inkoopbeleid
- Leveranciersmanagement
- Verhogen awareness onder betrokken medewerkers
- Reeds verzamelen van benodigde informatie voor:
 - Uitvoeren DPIA
 - Data-inventarisatie verwerkingsregister

PRIVACYCOMPANY 

Vorbereiding DPIA

Do's & Don'ts

Proces



© Claudia Quelle

Informatie

Typen informatie

- Dataclassificatie geeft op hoofdlijnen risico al aan
- Bij ontbreken van dataclassificatie geeft het soort informatiebeveiligingsbeleid een indicator
- Risico gekoppeld aan type informatie

Risico's bij informatie

- Gevoelige gegevens
- Hoeveelheid gegevens
- Wie heeft toegang?
- Unieke identificatie
- Mogelijkheid koppelen met andere gegevens

Risico's

Uitgangspunt bij beoordelen risico's =

het risico/de impact voor betrokkenen!

	Kans Laag	Kans Middel	Kans Hoog
Impact Laag	Risico Zeer Laag	Risico laag	Risico Middel
Impact Middel	Risico Laag	Risico Middel	Risico hoog
Impact Hoog	Risico Middel	Risico Hoog	Risico Zeer Hoog

Vergaren van informatie

Extern/leverancier applicatie

- Overeenkomst (SLA's)
- Beveiligingsmaatregelen (ISO/BIO)
- Gebruikershandleiding
 - Beheerder
 - Medewerker
- Gebruik van algoritme(n)!!
- LET OP: de verwerker = verplicht medewerking te verlenen!

Intern

- Procesbeschrijving
- Beleidsstukken
- Overeenkomsten
- Werkinstructies
- Autorisatiematrix (incl. beleid)

Aan de slag:

- Bespreek met elkaar vanuit het oogpunt van de wegbeheerder en de leverancier:
 - Welke relevante documentatie/informatie hebben jullie nodig voor een DPIA op één iVRI-applicatie (ITS-, TLC en RIS-functionaliteit)?
 - Welke afspraken maken jullie over het aanleveren van die informatie in de DPIA?
 - Welke afspraken maken jullie over het gebruik van die informatie in de DPIA?

PRIVACYCOMPANY 

DPIA

Beschrijving feitelijke situatie

Deel A

1. Het beschrijven van de persoonsgegevens die worden **verwerkt (of uitgewisseld)** (visualiseer gegevensstromen!)
2. Het beschrijven van de **gegevensverwerkingen**- en eventuele verstrekkingen.
3. Het beschrijven van de **doeleinden** van de gegevensverwerkingen
4. Het beschrijven van de **betrokken partijen**, inclusief **rollen** en **belangen**
5. Het beschrijven van de **verwerkingslocaties** (cloud, binnen de EER)
6. Het beschrijven van de **methoden en technieken**, de toepasselijke applicatie(s) en beveiligingsmaatregelen
7. Het beschrijven van **het juridisch kader**! Let hierbij met name op het reeds verzamelen van de informatie t.b.v. de juridische verantwoording!
8. Het beschrijven van de **bewaartermijnen** voor de verwerking

Beschrijving kenmerken gegevensverwerkingen

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Beschrijf de voorgenomen
gegevensverwerking

Beschrijving kenmerken persoonsgegevens

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Benoem alle categorieën persoonsgegevens en de relevante groepen betrokkenen. Deel de persoonsgegevens in in de categorieën:

- Gewoon
- Bijzonder
- Strafrechtelijk
- Wettelijk identificerend

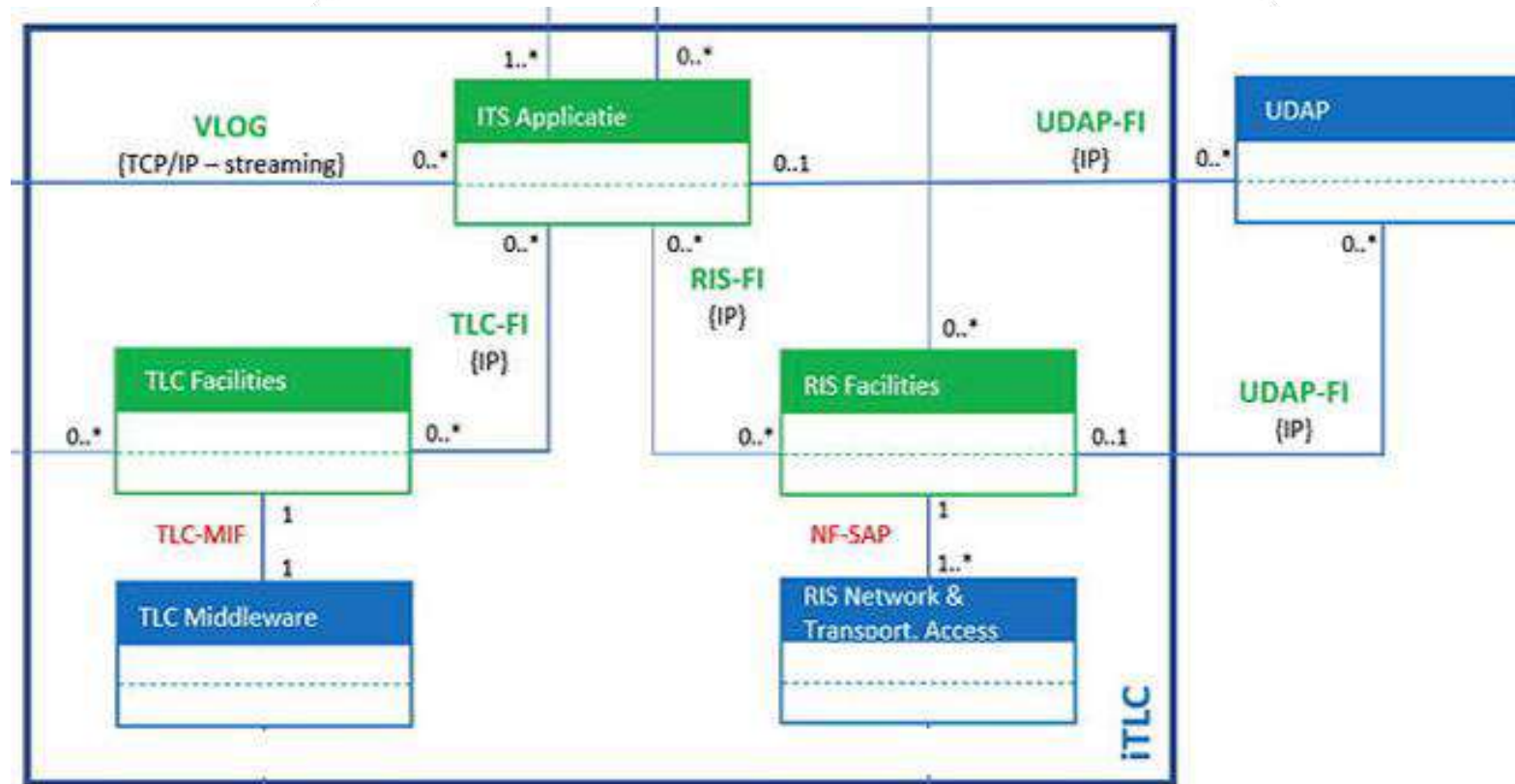
Beschrijving van de te verwerken persoonsgegevens

- Wat zijn persoonsgegevens?
- Wat is verwerken?

Verzamelen van informatie en beschrijven van de applicatie/datastroom en functionaliteiten:

- Welke persoonsgegevens worden verwerkt (*tip: beschrijf alle data*); en
- Beschrijf hierbij zowel:
 - De data die een iVRI ontvangt
 - De data die een iVRI verwerkt inclusief combineren/koppelen van de data (= ook een verwerking)
 - De data die een iVRI verstuurt
- Visualiseer dit in een Dataflowdiagram

Beschrijving van de te verwerken persoonsgegevens



Voorbeelden

CAM, SRM en SSM data:

Vehicle ID (SRM/SSM)
BasicVehicleRole (SRM/SSM)
StationID (CAM)
VehicleType (SRM/SSM)

V-log:

<vri_id> en <datum / tijd> aanduiding

BIT	15 (MSB)	12	10 - 8	7 - 0 (LSB)
BETEKENIS	Richting	Status	Type	Snelheid

Let op: uitspraak van
20 december 2023
Raad van State

Beschrijving kenmerken gegevensverwerkingen

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Omschrijf de voorgenomen
gegevensverwerkingen

Beschrijven van de gegevensverwerking

- Welke handelingen (= verwerkingen) vinden er plaats?
- Beschrijf in de DPIA welke verwerkingen plaatsvinden:
 - Bijvoorbeeld op basis van de use cases
 - Prioriteren
 - Informeren
 - Optimaliseren
 - En op basis van de iVRI-faciliteiten:
 - TLC- faciliteit
 - ITS- faciliteit
 - RIS- faciliteit
- Vul dit (indien gewenst) aan in de Dataflowdiagram



**Relatie met
grondslag en
doeleinden!!**

Beschrijven van de gegevensverwerking

Voorbeelden van gegevensverwerkingen?

- het verwerken van een Pseudo-ID middels CAM en SRM berichten voor het verlenen van prioriteit
- het verwerken van de data ten behoeve van het optimaliseren van het verkeersaanbod ten behoeve van het wegverkeer en de verkeersveiligheid
- het verwerken van een Pseudo-ID middels SRM en SSM berichten voor het informeren van weggebruikers dan wel prioriteitsgerechtigde voertuigen
- het verwerken van gegevens van medewerkers wegbeheerder ten behoeve van accountbeheer en toegang tot de iVRI-applicatie(s)

Beschrijven van de gegevensverwerking

Voorbeeld t.b.v. beschrijven gegevensverwerking

Om het prioriteitsverzoek van een lijnbus 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.

Beschrijving kenmerken verwerkingsdoeleinden

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Beschrijf de verwerkingsdoeleinden

Beschrijven van de doeleinden van de verwerking

Beschrijf de doeleinden op basis van:

- Wet- en regelgeving wegbeheerder (art. 2 Wegenverkeerswet);
- Relevante use cases (optimaliseren, prioriteren en informeren); én
- Eventuele aanvullende doeleinden

Beschrijven van de doeleinden van de verwerking

Voorbeeld

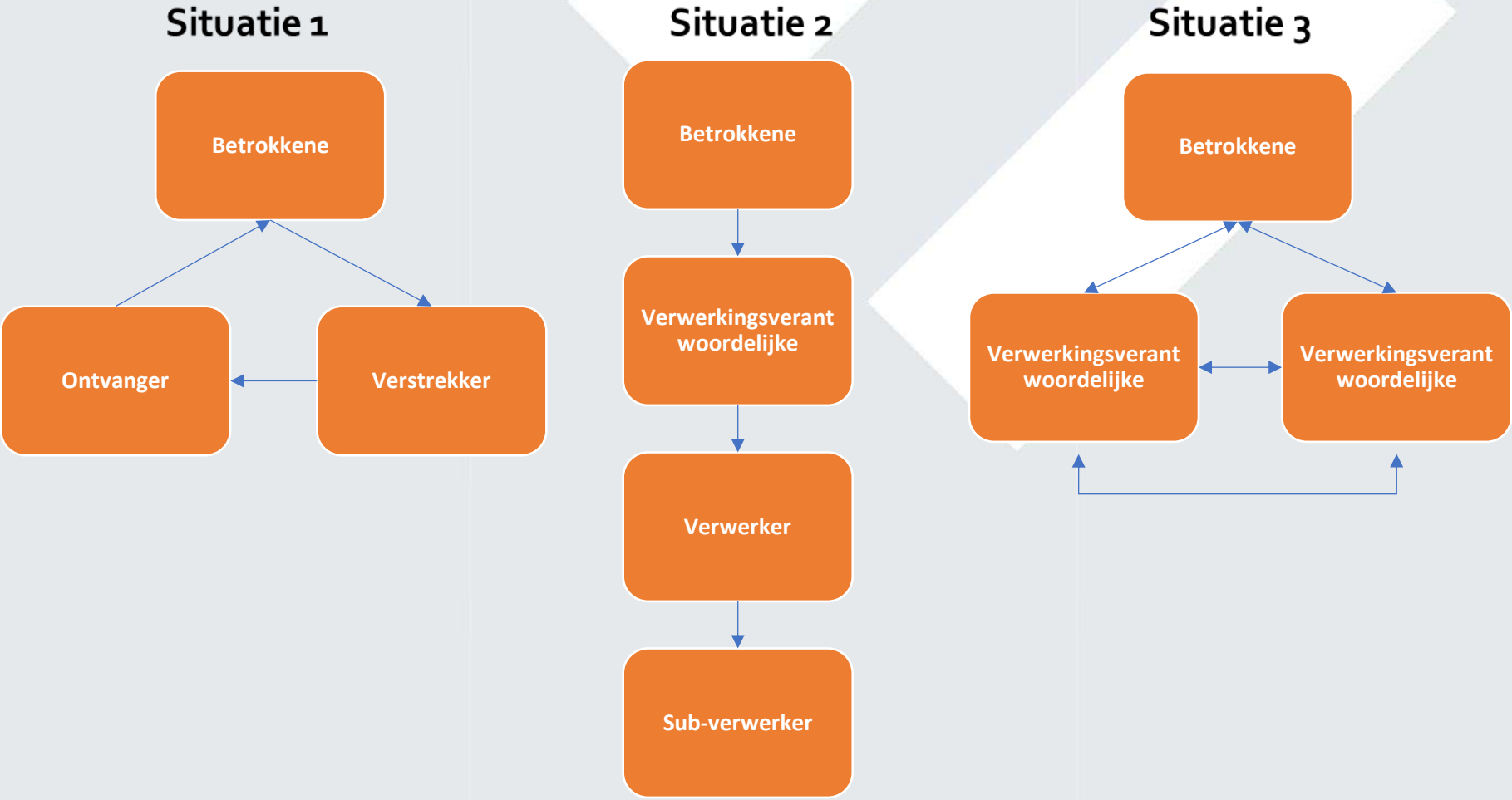
- Het verhogen van verkeersveiligheid ten behoeve van nood- en hulpdiensten bij het passeren van iVRI's.
- Het optimaliseren van de verkeersafwikkeling door het verbeterd laten presteren van kruispunten en verkeersdoorstroming;
- Het verkorten van de reistijd voor openbaar vervoer en verbeteren van stiptheid en regelmaat van de dienstregeling;
- Het beperken van het aantal stops van vrachtverkeer middels vlottere verkeersafwikkelingen en daarmee het beperken van uitstoot en verbeteren van leefbaarheid, en bespoedigen van de goederenafwikkeling.

Beschrijving kenmerken betrokken partijen

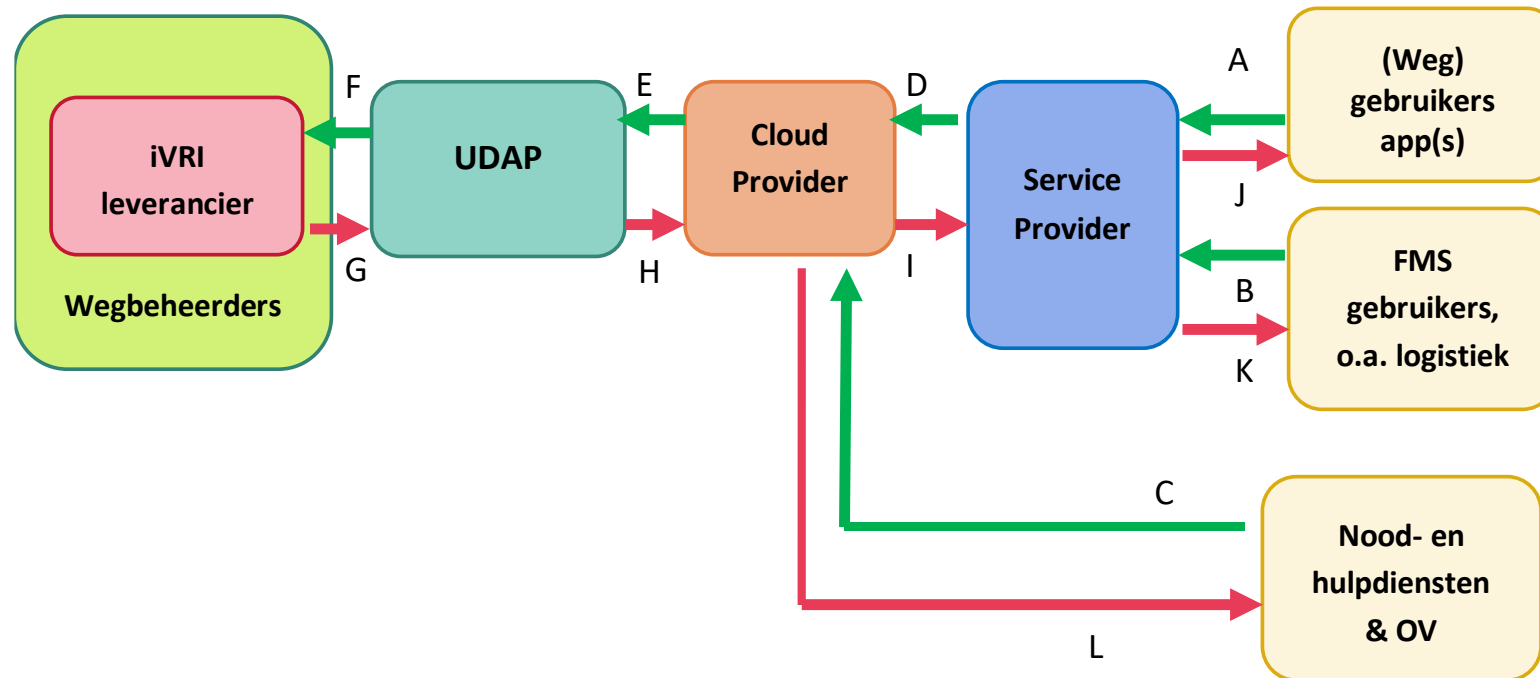
1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Benoem de betrokken organisaties, welke functionarissen toegang hebben tot de persoonsgegevens en welke rollen deze organisaties hebben:

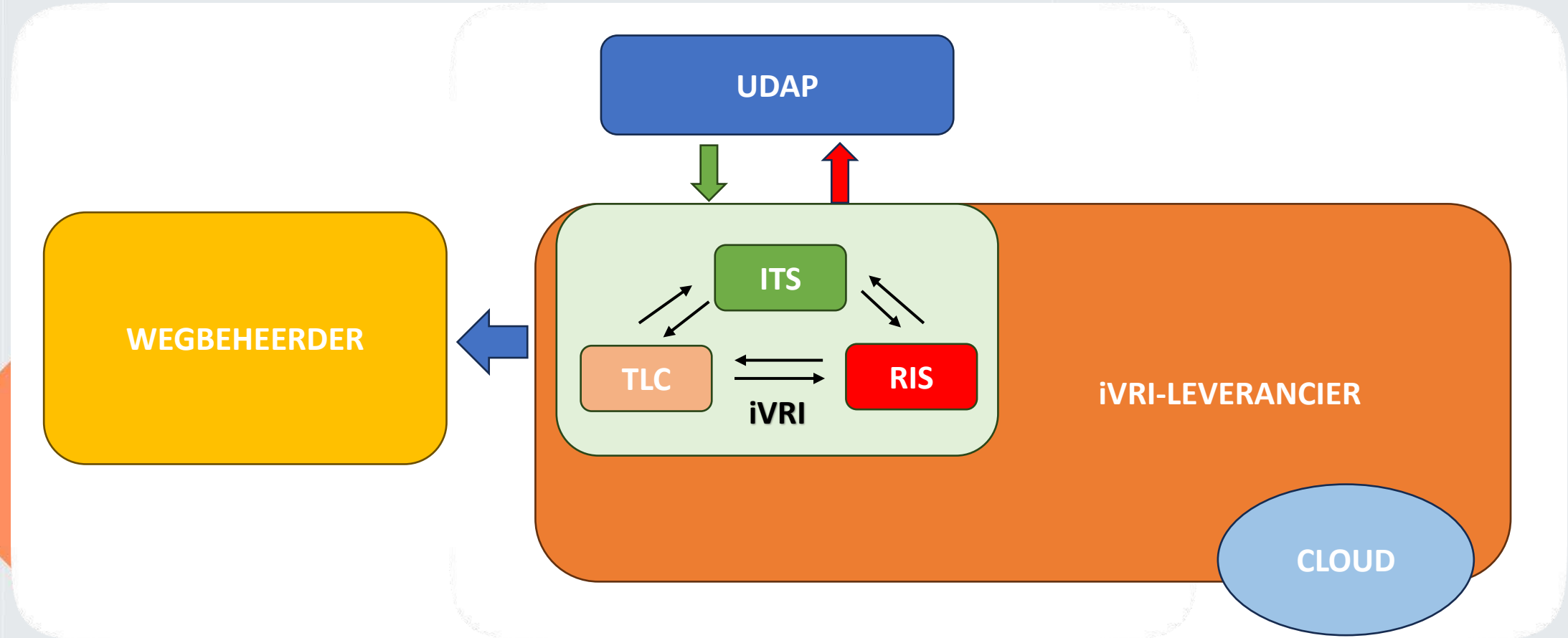
- Verwerkingsverantwoordelijke
- Verwerker
- Verstrekker
- Ontvanger



Keten Talking Traffic



Rol wegbeheerder en iVRI-leverancier(s)



Beschrijving kenmerken belangen van partijen

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Beschrijf de belangen van de betrokken partijen.

Beschrijving kenmerken verwerkingslocaties

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Waar worden de persoonsgegevens verwerkt?

Beschrijving kenmerken technieken en methode(n)

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Beschrijf de technische middelen en methoden waar de gegevensverwerking uit bestaat

Technieken en methoden van de verwerkingen

Beschrijf hier de:

- Technische werking van de iVRI-applicatie(s)
 - Wijze waarop wordt voldaan aan normering als ISO:27001 en/of Baseline Informatiebeveiliging Overheid (BIO)
 - Autorisaties (zowel leverancier(s) als medewerkers wegbeheerder)
 - Logging
 - (extra) functionaliteiten van de applicatie (o.a. rapportage-functionaliteit)
 - Verwijderen van de data
 - Koppelingen met andere databases/API's
 - Opslag van de gegevens inclusief back-ups
- Het gebruik van een algoritme (en werking hiervan inclusief toets gelet op impact mensenrechten (Impact Assessment Mensenrechten en Algoritmes))

Beschrijving kenmerken juridisch en beleidsmatig kader

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Is er (sectorspecifieke) wet- en regelgeving van toepassing?

Beschrijving kenmerken bewaartermijnen

1. Voorstel
2. Persoonsgegevens
3. Gegevensverwerkingen
4. Verwerkingsdoeleinden
5. Betrokken partijen
6. Belangen bij de gegevensverwerking
7. Verwerkingslocaties
8. Techniek en methode van gegevensverwerking
9. Juridisch en beleidsmatig kader
10. Bewaartermijnen

Bepaal en motiveer bewaartermijnen

Beschrijven bewaar- en vernietigingstermijnen/-beleid

Hoe wordt voldaan aan het principe van opslagbeperking?

- Persoonsgegevens mogen niet langer worden bewaard dan nodig/toegestaan;
- Heb je persoonsgegevens niet meer nodig of vernietigen vanwege wet-/regelgeving = vernietigen/wissen inclusief back-ups!
- Anonimiseren = ook een maatregel om te voldoen aan opslagbeperking!
 - Niet meer direct of indirect herleidbaar zijn tot personen ≠ persoonsgegeven dus AVG niet (meer) van toepassing

PRIVACYCOMPANY 

DPIA

Beschrijving juridische verantwoording

Deel B

1. Het beschrijven van de **grondslagen** van de gegevensverwerking (eventueel ook de gegevensuitwisseling en – verstrekking door ketenpartners)
2. Het beschrijven van de **doelbinding**, en met name beschrijven of er sprake is van verdere verwerking
3. Indien relevant – beschrijven van **bijzondere of gevoelige persoonsgegevens** en rechtmatige grondslag voor de (verdere) verwerking
4. Het beschrijven (en toetsen) van de **noodzakelijkheid** van de gegevensverwerking (**BELANGRIJK**)
5. Het beschrijven van de wijze waarop de **betrokkenen hun rechten kunnen uitoefenen**.

Beschrijven juridische verantwoording

Basis voor het rechtmatig verwerken van (i)VRI-data is: art. 2 Wegenverkeerswet!

- het verzekeren van de veiligheid op de weg;
- het beschermen van weggebruikers en 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.

Beoordelen of wordt voldaan aan de eisen van:

- Proportionaliteit en
- Subsidiariteit

Belangrijk is dat:

CAM en SRM data enkel voor het doel van het optimaliseren van de regeling van de iVRI's, respectievelijk de invulling van de prioriteitsfacilitering wordt gebruikt! Dit conform de Wegenverkeerswet (doelen) en iVRI-specificaties

PRIVACYCOMPANY 

DPIA

Beschrijving risico's & maatregelen

Deel C

1. Het beschrijven van de risico's (voor betrokkenen). Ga hierbij uit van géén maatregelen (dit om alle maatregelen correct te beschrijven).
2. Het inschatten van de risico's gelet op impact (op de betrokkene) en kans dat het risico zich voordoet

Beschrijven van de risico's

- Er is geen volledige checklist voor risico's
- Risico's voor de betrokkenen, niet voor de verantwoordelijke
- Niet kunnen voldoen aan rechten van betrokkenen is ook een risico
- Betrek zoveel mogelijk perspectieven
- Inventariseer zoveel mogelijk risico's voordat je de maatregelen beschrijft.

Voorbeelden van Risico's

- Te lang bewaren van StationID's (CAM)/Vehicle ID's (RIS)
- Te lang bewaren (overige) data door wegbeheerder
- Onrechtmatig verder verwerken van data door wegbeheerder
- Toegang tot data in private domein Talking Traffic keten door iVRI-leverancier
- Geen verwerkersovereenkomst of onjuiste afspraken
- Opslag van data buiten EER (EU) zonder correcte waarborgen
- Verstrekken van iVRI-data door wegbeheerder (zonder grondslag)
- Geen of niet passende beveiligingsmaatregelen iVRI-faciliteiten/applicatie

Deel D

1. Het per risico beschrijven van de maatregelen om het risico te minimaliseren of te beperken tot (laag)
2. Het beschrijven van de uitkomsten van de risico's na het treffen van de maatregelen (samenvatting).

Beschrijven van de maatregelen

De maatregelen om de geconstateerde risico's te beperken/minimaliseren:

- (informatie)beveiligingsmaatregelen:
 - Informatiebeveiliging conform ISO:27001 en BIO?
 - Autorisaties
 - Logging
 - Back-ups
- Data-minimalisatie
- Verwerkersovereenkomst
- Opslagbeperking (= bewaar- en vernietigingstermijn)
- Informeren betrokkenen?

PRIVACYCOMPANY 

DPIA

Praktische tips & aandachtspunten

6 Praktische tips

- 1) Scope helder bepalen
- 2) Focus houden
- 3) Perspectief betrokkene
- 4) Beoordeel alsof er nog geen maatregelen zijn getroffen
- 5) Zorg voor een duidelijke procesbeschrijving en een datastroombiagram (DFD)
- 6) Trek een heldere conclusie

Aandachtspunten

- Altijd belangrijk om de juiste en volledige informatie te verkrijgen/verzamelen (ook i.v.m. inventarisatie)
- Algemene awareness is essentieel om juiste medewerking te verkrijgen van collega's
- Belang is groot, want: een organisatie moet haar handelen goed kunnen verantwoorden! En een DPIA en risicoanalyse helpen daarbij

Aandachtspunten

- Wees streng
- Begin op tijd
- Is voorgestelde plan ook het beste plan?
- Wat is ideaalbeeld vanuit privacyperspectief en in hoeverre past dat bij praktijkwensen?
- Wat zijn mitigerende maatregelen?

Privacy Company B.V.

bas.bekenkamp@privacycompany.nl

+31(0)6 46 99 53 95