

Richtsnoeren



Richtsnoeren 01/2020 inzake de verwerking van persoonsgegevens in het kader van verbonden voertuigen en mobiliteitsgerelateerde toepassingen

Versie 2.0

Vastgesteld op 9 maart 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versiegeschiedenis

Versie 2.0	9 maart 2021	Vaststelling van de richtsnoeren na openbare raadpleging
Versie 1.0	28 januari 2020	Vaststelling van de richtsnoeren voor openbare raadpleging

1	INLEIDING	4
1.1	Aanverwante werkzaamheden	5
1.2	Toepasselijk recht.....	7
1.3	Toepassingsgebied	8
1.4	Definities.....	12
1.5	Risico's met betrekking tot de persoonlijke levenssfeer en gegevensbescherming.....	13
2	ALGEMENE AANBEVELINGEN	16
2.1	Categorieën gegevens	16
2.2	Doeleinden	18
2.3	Relevantie en minimale gegevensverwerking.....	18
2.4	Gegevensbescherming door ontwerp en door standaardinstellingen	19
2.5	Informatie.....	23
2.6	Rechten van de betrokkene	25
2.7	Beveiliging	26
2.8	Doorzending van persoonsgegevens aan derden	27
2.9	Doorgifte van persoonsgegevens buiten de EU/EER	27
2.10	Gebruik van wifitechnologieën aan boord van voertuigen.....	27
3	CASESTUDY'S	28
3.1	Verlening van een dienst door een derde.....	28
3.2	eCall	32
3.3	Bestudering van oorzaken en gevolgen van ongevallen	35
3.4	Bestrijding van autodiefstal.....	38

Gezien artikel 70, lid 1, punt e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna “AVG” genoemd),

Gezien de EER-Overeenkomst en in het bijzonder bijlage XI en Protocol 37 daarbij, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018¹,

Gezien de artikelen 12 en 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 INLEIDING

1. De auto, een symbool van de economie van de twintigste eeuw, is een massaconsumptieproduct dat de samenleving als geheel heeft beïnvloed. Mensen associëren auto's vaak met vrijheid en zien hun auto als meer dan slechts een vervoermiddel.

Auto's bieden immers een zekere mate van autonomie in de privésfeer, zonder inmenging van buitenaf. Nu verbonden voertuigen steeds meer gemeengoed worden, sluit die visie niet langer aan op de realiteit. De connectiviteit in voertuigen breidt zich snel uit van luxemodellen en -merken tot grootschalig geproduceerde middenklassemodellen, en voertuigen worden knooppunten waar een grote hoeveelheid gegevens samenkomt. Niet alleen voertuigen, maar ook bestuurders en passagiers zijn in steeds sterkere mate verbonden. Tal van modellen die de afgelopen jaren in de handel zijn gebracht, zijn uitgerust met sensoren en verbonden boordapparatuur, die onder meer de motorprestaties, de rijgewoonten, de bezochte locaties en mogelijk zelfs de oogbewegingen van de bestuurder, zijn of haar polsslag of biometrische gegevens kunnen verzamelen en registreren om een natuurlijke persoon te identificeren².

2. Deze gegevensverwerking vindt plaats binnen een complex ecosysteem waarin niet alleen de traditionele spelers van de auto-industrie een rol spelen, maar dat ook wordt gevormd door opkomende nieuwe spelers in de digitale economie. Deze nieuwe spelers kunnen infotainmentdiensten aanbieden, zoals onlinemuziek, informatie over de toestand van de wegen en verkeersinformatie, of rijassistentiesystemen en -diensten, zoals software voor de automatische piloot, updates over de toestand van het voertuig, op het gebruik gebaseerde verzekeringen of dynamische cartografie. Aangezien voertuigen via elektronische-communicatienetwerken met elkaar verbonden zijn, spelen ook de bij dit proces betrokken weginfrastructuurbeheerders en telecombedrijven een belangrijke rol met betrekking tot de mogelijke verwerking van de persoonsgegevens van bestuurders en passagiers.
3. Verbonden voertuigen genereren bovendien steeds grotere hoeveelheden gegevens, waarvan de meeste als persoonsgegevens kunnen worden beschouwd omdat zij betrekking hebben op bestuurders of passagiers. Zelfs indien de door een verbonden auto verzamelde

¹ Verwijzingen naar “lidstaten” in dit document moeten worden gelezen als verwijzingen naar “lidstaten van de EER”.

² Infografiek “Data and the connected car” (gegevens en de verbonden auto) van het Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

gegevens niet rechtstreeks zijn gekoppeld aan een naam, maar aan technische aspecten en kenmerken van de auto, zullen zij betrekking hebben op de bestuurder of de passagiers. Om een voorbeeld te geven: gegevens over de rijstijl of de afgelegde afstand, gegevens over de slijtage van voertuigonderdelen, locatiegegevens of door camera's verzamelde gegevens kunnen betrekking hebben op het rijgedrag, maar ook informatie bevatten over andere personen die zich mogelijk in het voertuig bevinden of over betrokkenen die langsrijden. Deze technische gegevens worden geproduceerd door een natuurlijke persoon en maken het mogelijk dat hij/zij direct of indirect wordt geïdentificeerd door de verwerkingsverantwoordelijke of door iemand anders. Een voertuig kan worden gezien als een terminal die door verschillende gebruikers kan worden gebruikt. Net als bij een pc doet het feit dat er mogelijk meerdere gebruikers zijn, geen afbreuk aan het persoonlijke karakter van de gegevens.

4. In 2016 organiseerde de Fédération Internationale de l'Automobile (FIA) de Europese campagne "My Car My Data", om erachter te komen hoe Europeanen denken over verbonden auto's³. De campagne maakte niet alleen duidelijk dat bestuurders veel belangstelling hebben voor connectiviteit, maar ook dat waakzaamheid geboden is bij het gebruik van de door voertuigen geproduceerde gegevens en hoe belangrijk het is de wetgeving inzake de bescherming van persoonsgegevens na te leven. De uitdaging voor alle belanghebbenden is dus om de dimensie van "bescherming van persoonsgegevens" al in de productontwerpfase te integreren, en ervoor te zorgen dat autogebruikers transparantie genieten met betrekking tot en controle uitoefenen over hun gegevens overeenkomstig overweging 78 van de AVG. Een dergelijke aanpak helpt het vertrouwen van de gebruiker te versterken, en daarmee de ontwikkeling van de technologieën op lange termijn.

1.1 Aanverwante werkzaamheden

5. Verbonden voertuigen zijn de afgelopen tien jaar een belangrijk onderwerp geworden voor regulerende instanties, met name de laatste paar jaren. Zo zijn er verschillende nationale en internationale documenten gepubliceerd over de beveiliging en privacy van verbonden voertuigen. Deze regels en initiatieven hebben tot doel de bestaande kaders voor gegevensbescherming en privacy aan te vullen met sectorspecifieke regels of richtsnoeren voor professionals.

1.1.1 Europese en internationale initiatieven

6. Sinds 31 maart 2018 is een op het alarmnummer 112 gebaseerd eCall-boordsysteem verplicht voor alle nieuwe voertuigen uit de klassen M1 en N1 (personenauto's en lichte bedrijfsvoertuigen).⁴⁵ In 2006 had de Groep gegevensbescherming artikel 29 reeds een werkdocument betreffende de gevolgen van het eCall-initiatief vanuit het oogpunt van bescherming van gegevens en van de persoonlijke levenssfeer goedgekeurd⁶. Bovendien heeft de Groep gegevensbescherming artikel 29, zoals eerder besproken, in oktober 2017 een advies aangenomen over de verwerking van persoonsgegevens in het kader van coöperatieve intelligente vervoerssystemen (C-ITS).
7. In januari 2017 heeft het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) een studie over de cyberbeveiliging en -weerbaarheid van slimme auto's gepubliceerd. Die studie bevat een overzicht van de gevoelige activa en de bijbehorende bedreigingen, risico's,

³ Campagne "My Car My Data" (mijn auto, mijn gegevens); <http://www.mycarmydata.eu/>

⁴ De interoperabele EU-brede eCall; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

⁵ Besluit nr. 585/2014/EU van het Europees Parlement en de Raad van 15 mei 2014 inzake de uitrol van de interoperabele eCall-dienst in de hele EU (Voor de EER relevante tekst); <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32014D0585>

⁶ Werkdocument betreffende de gevolgen van het eCall-initiatief vanuit het oogpunt van bescherming van gegevens en van de persoonlijke levenssfeer; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_nl.pdf

verzachtende factoren en mogelijke uit te voeren beveiligingsmaatregelen⁷. In september 2017 heeft de internationale conferentie van commissarissen voor de bescherming van gegevens en de persoonlijke levenssfeer (ICDPPC) een resolutie aangenomen over verbonden voertuigen⁸. Tot slot heeft de internationale werkgroep inzake gegevensbescherming bij telecommunicatie (IWGDPT) in april 2018 een werkdocument aangenomen over verbonden voertuigen⁹.

1.1.2 Nationale initiatieven van leden van het Europees Comité voor gegevensbescherming (EDPB)

8. In januari 2016 hebben de conferentie van de Duitse federale en deelstaatautoriteiten voor gegevensbescherming en de Duitse vereniging van de automobielsector (VDA) een gemeenschappelijke verklaring gepubliceerd over de beginselen van gegevensbescherming in verbonden en niet-verbonden voertuigen¹⁰. In augustus 2017 heeft het Centre for Connected and Autonomous Vehicles (centrum voor verbonden en zelfrijdende voertuigen, CCAV) van het Verenigd Koninkrijk een gids uitgebracht met de beginselen inzake de cyberbeveiliging van verbonden en geautomatiseerde voertuigen, om de bewustwording hierover in de automobielsector te vergroten¹¹. In oktober 2017 heeft de Franse gegevensbeschermingsautoriteit, de Commission Nationale de l'Informatique et des Libertés (CNIL), een nalevingspakket voor verbonden auto's gepubliceerd om belanghebbenden te helpen bij het integreren van gegevensbescherming door ontwerp en door standaardinstellingen, zodat betrokkenen effectieve controle kunnen uitoefenen over hun gegevens¹².

⁷ Cyberbeveiliging en -weerbaarheid van slimme auto's: <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

⁸ Resolutie over gegevensbescherming in geautomatiseerde en verbonden voertuigen; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

⁹ Werkdocument over verbonden voertuigen: <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>

¹⁰ Gegevensbeschermingsaspecten van het gebruik van verbonden en niet-verbonden voertuigen; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

¹¹ Beginselen inzake de cyberbeveiliging van verbonden en geautomatiseerde voertuigen; <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

¹² Nalevingspakket voor een verantwoord gebruik van gegevens in verbonden auto's; <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>

1.2 Toepasselijk recht

9. De AVG vormt in dezen het EU-rechtskader. De AVG is van toepassing wanneer de verwerking van persoonsgegevens in het kader van verbonden voertuigen gepaard gaat met de verwerking van persoonsgegevens van natuurlijke personen.
10. Naast de AVG bevat Richtlijn 2002/58/EG, zoals herzien bij Richtlijn 2009/136/EG (de “e-privacyrichtlijn”), **een specifieke norm voor alle actoren die informatie willen opslaan of inzien die is opgeslagen in de eindapparatuur van een abonnee of gebruiker in de Europese Economische Ruimte (EER).**
11. De meeste bepalingen van de e-privacyrichtlijn (zoals de artikelen 6 en 9) zijn alleen van toepassing op aanbieders van openbare elektronische-communicatiediensten en op aanbieders van openbare communicatienetwerken, maar artikel 5, lid 3, van de e-privacyrichtlijn is een algemene bepaling. Zij is niet alleen van toepassing op elektronische-communicatiediensten, maar ook op elke particuliere of openbare entiteit die informatie op een eindapparaat plaatst of daaruit afleest, ongeacht de aard van de gegevens die worden opgeslagen of geraadpleegd.
12. Het begrip “eindapparatuur” wordt gedefinieerd in Richtlijn 2008/63/EG¹³. In artikel 1, punten a) en b), wordt eindapparatuur omschreven als: *“a) de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar telecommunicatienet zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een aansluiting is indirect wanneer een apparaat geplaatst is tussen het eindapparaat en de interface van het net; b) satellietgrondstationapparatuur”*.
13. Bijgevolg moeten het verbonden voertuig en de daarop aangesloten apparatuur, mits aan de bovengenoemde criteria is voldaan, worden beschouwd als “eindapparatuur” (net als een computer, een smartphone of een smart-tv) en zijn de bepalingen van artikel 5, lid 3, van de e-privacyrichtlijn in voorkomend geval van toepassing.
14. Zoals de EDPB in zijn advies 5/2019 over de wisselwerking tussen de e-privacyrichtlijn en de AVG¹⁴ heeft uiteengezet, bepaalt artikel 5, lid 3, van de e-privacyrichtlijn dat in de regel, en met inachtneming van de in punt 17 verderop genoemde uitzonderingen op die regel, voorafgaande toestemming vereist is voor het opslaan van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker. Voor zover de informatie die in de apparatuur van de eindgebruiker is opgeslagen uit persoonsgegevens bestaat, heeft artikel 5, lid 3, van de e-privacyrichtlijn voorrang boven artikel 6 AVG wat betreft het opslaan van of verkrijgen van toegang tot deze informatie¹⁵. Wil de latere verwerking van persoonsgegevens na de voornoemde verwerking, met inbegrip van persoonsgegevens die zijn verkregen door toegang tot de informatie in de eindapparatuur, rechtmatig zijn, dan moet deze ook een rechtsgrond hebben krachtens artikel 6 AVG¹⁶.
15. Aangezien de verwerkingsverantwoordelijke, wanneer hij/zij toestemming vraagt voor het opslaan van of het verkrijgen van toegang tot informatie overeenkomstig artikel 5, lid 3, van de e-privacyrichtlijn, de betrokkene moet informeren over alle doeleinden van de verwerking

¹³ Richtlijn 2008/63/EG van de Commissie van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur (Gecodificeerde versie) (Voor de EER relevante tekst); <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32008L0063>

¹⁴ Europees Comité voor gegevensbescherming, Advies 5/2019 over de wisselwerking tussen de e-privacyrichtlijn en de algemene verordening gegevensbescherming, met name wat betreft de taken en bevoegdheden van gegevensbeschermingsautoriteiten, aangenomen op 12 maart 2019, punt 40.

¹⁵ Ibid., punt 40.

¹⁶ Ibid., punt 41.

— met inbegrip van de verwerking na de hierboven genoemde verwerkingen (d.w.z. de “daaropvolgende verwerking”) — is toestemming op grond van artikel 6 AVG over het algemeen de meest geschikte rechtsgrond voor de verwerking van persoonsgegevens na dergelijke verwerkingen (voor zover het doel van de daaropvolgende verwerking onder de toestemming van de betrokkene valt, zie punten 53 en 54 hieronder). Toestemming zal dus waarschijnlijk de rechtsgrond vormen voor zowel het opslaan van en het verkrijgen van toegang tot reeds opgeslagen informatie als de daaropvolgende verwerking van persoonsgegevens¹⁷. Bij de beoordeling van de naleving van artikel 6 AVG moet er rekening mee worden gehouden dat de verwerking als geheel gepaard gaat met specifieke activiteiten waarvoor de EU-wetgever extra bescherming heeft willen bieden¹⁸. Bovendien moeten verwerkingsverantwoordelijken rekening houden met de impact op de rechten van de betrokkene wanneer zij de passende rechtsgrond vaststellen, om zo het beginsel van behoorlijkheid te eerbiedigen¹⁹. Het komt erop neer dat verwerkingsverantwoordelijken artikel 6 AVG niet kunnen invoeren om de aanvullende bescherming die wordt geboden door artikel 5, lid 3, van de e-privacyrichtlijn, te verminderen.

16. De EDPB herinnert eraan dat toestemming in de e-privacyrichtlijn dezelfde betekenis behoudt als in de AVG en moet voldoen aan alle vereisten voor toestemming die zijn opgenomen in artikel 4, punt 11, en artikel 7 AVG.
17. Hoewel toestemming het beginsel is, kan volgens artikel 5, lid 3, van de e-privacyrichtlijn de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur, worden vrijgesteld van het vereiste van geïnformeerde toestemming, indien wordt voldaan aan een van de volgende criteria:
 -) **Vrijstelling 1:** opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk;
 -) **Vrijstelling 2:** wanneer opslag of toegang strikt noodzakelijk is, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.
18. In dergelijke gevallen is de verwerking van persoonsgegevens, waaronder persoonsgegevens die zijn verkregen door zich toegang te verschaffen tot informatie in de eindapparatuur, gebaseerd op een van de rechtsgronden van artikel 6 AVG. Toestemming is bijvoorbeeld niet nodig wanneer de gegevensverwerking noodzakelijk is om door de betrokkene gevraagde GPS-navigatiediensten te verlenen wanneer dergelijke diensten kunnen worden aangemerkt als diensten van de informatiemaatschappij.

1.3 Toepassingsgebied

19. De EDPB wijst erop dat deze richtsnoeren bedoeld zijn om een correcte verwerking van persoonsgegevens door een breed scala van belanghebbenden die op dit gebied werkzaam zijn, te vergemakkelijken. Zij zijn echter niet bedoeld om alle mogelijke gebruikssituaties in deze context te bestrijken of om richtsnoeren te geven voor elke mogelijke specifieke situatie.
20. Dit document is met name gericht op de verwerking van persoonsgegevens in verband met het niet-beroepsmatige gebruik van verbonden voertuigen door betrokkenen, zoals

¹⁷ De toestemming die wordt vereist door artikel 5, lid 3, van de e-privacyrichtlijn en de toestemming die nodig is als rechtsgrond voor de verwerking van gegevens (artikel 6 AVG) voor hetzelfde specifieke doel, kunnen tegelijkertijd worden verkregen (bijvoorbeeld door een vakje aan te vinken waarin duidelijk wordt aangegeven waarmee de betrokkene instemt).

¹⁸ Advies 5/2019, punt 41.

¹⁹ Europees Comité voor gegevensbescherming, Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, versie 2.0, 8 oktober 2019, punt 1.

bestuurders, passagiers, voertuigeigenaren, andere weggebruikers enz. Meer specifiek gaat het om de persoonsgegevens die: i) worden verwerkt in het voertuig, ii) worden uitgewisseld tussen het voertuig en de daarmee verbonden persoonlijke apparaten (bijvoorbeeld de smartphone van de gebruiker) of iii) lokaal in het voertuig worden verzameld en voor verdere verwerking worden geëxporteerd naar externe partijen (zoals voertuigfabrikanten, infrastructuurbeheerders, verzekeringsmaatschappijen, autoreparateurs).

21. De definitie van “verbonden voertuig” moet in dit document ruim worden opgevat. Een verbonden voertuig kan worden gedefinieerd als een voertuig dat is uitgerust met een groot aantal elektronische regeleenheden die met elkaar zijn verbonden via een netwerk aan boord van het voertuig, alsmede connectiviteitsvoorzieningen die het mogelijk maken informatie uit te wisselen met andere apparaten zowel binnen als buiten het voertuig. Zo kunnen gegevens worden uitgewisseld tussen het voertuig en de daarmee verbonden persoonlijke apparaten, waardoor bijvoorbeeld mobiele toepassingen kunnen worden gespiegeld aan de informatie- en entertainmentmodule in het dashboard van de auto. Ook de ontwikkeling van autonome mobiele toepassingen, d.w.z. toepassingen die losstaan van het voertuig (waarbij bijvoorbeeld alleen de smartphone wordt gebruikt) en die bestuurders bijstaan, valt binnen de reikwijdte van dit document, aangezien zij bijdragen tot de verbindingmogelijkheden van het voertuig, ook al berust de werking ervan niet noodzakelijkerwijs op de uitwisseling van gegevens met het voertuig. Er zijn tal van uiteenlopende toepassingen voor verbonden voertuigen en ze kunnen het volgende omvatten²⁰:
22. *Mobiliteitsbeheer*: functies die bestuurders in staat stellen snel en kostenefficiënt hun bestemming te bereiken, door tijdig informatie te verstrekken over GPS-navigatie, potentieel gevaarlijke omgevingsfactoren (zoals ijzel), verkeersopstoppingen of wegwerkzaamheden, assistentie bij parkeerterreinen of -garages, geoptimaliseerd brandstofverbruik of rekeningrijden.
23. *Voertuigbeheer*: functies die bedoeld zijn om bestuurders te helpen de gebruikskosten te verlagen en het gebruiksgemak te vergroten, zoals een melding over de staat van het voertuig en onderhoudsherinneringen, de doorgifte van gebruiksgegevens (bijvoorbeeld voor voertuigreparatiediensten), aangepaste verzekeringen op basis van hoeveel en hoe je rijdt, bediening op afstand (bijvoorbeeld verwarmingssysteem) of profielconfiguraties (zoals de zitpositie).
24. *Verkeersveiligheid*: functies die de bestuurder waarschuwen voor externe gevaren en interne reacties, zoals bescherming tegen botsingen, waarschuwingen voor gevaren, waarschuwingen bij het verlaten van de rijstrook, detectie van slaperigheid bij de bestuurder, noodoproep (eCall) of “zwarte dozen” voor het onderzoeken van ongevallen (event data recorder).
25. *Amusement*: functies voor het informeren en entertainen van de bestuurder en de passagiers, zoals smartphone-interfaces (handsfree bellen, gesproken tekstberichten), WLAN-hotspots, muziek, video, internet, sociale media, mobiele kantoor diensten of diensten met betrekking tot intelligente huizen.
26. *Assistentie van de bestuurder*: functies waarbij het rijden geheel of gedeeltelijk wordt geautomatiseerd, zoals operationele assistentie of automatische piloot bij druk verkeer, bij het parkeren of op snelwegen.
27. *Welzijn*: functies die het comfort, de rijvaardigheid en de rijgeschiktheid van de bestuurder controleren, zoals detectie van vermoeidheid of medische bijstand.

²⁰ PwC Strategy 2014. “In the fast lane. The bright future of connected cars”:
https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

28. Voertuigen kunnen dus standaard verbonden zijn of niet en persoonsgegevens kunnen op verschillende manieren worden verzameld, onder meer via: i) voertuigsensoren, ii) telematicaboxen of iii) mobiele toepassingen (die bijvoorbeeld toegankelijk zijn via een apparaat van een bestuurder). Om binnen de reikwijdte van dit document te vallen, moeten mobiele toepassingen betrekking hebben op de rij-omgeving. Toepassingen op het gebied van GPS-navigatie vallen er bijvoorbeeld binnen. Toepassingen die als enige functie hebben om bestuurders te wijzen op interessante plaatsen (restaurants, historische monumenten enz.) vallen echter buiten de reikwijdte van deze richtsnoeren.
29. Veel van de gegevens die door een verbonden voertuig worden gegenereerd, hebben betrekking op een geïdentificeerde of identificeerbare natuurlijke persoon en vormen dus persoonsgegevens. Het gaat bijvoorbeeld om direct identificeerbare gegevens (zoals de volledige identiteit van de bestuurder), maar ook om indirect identificeerbare gegevens, zoals informatie over de afgelegde ritten, de gegevens over het voertuiggebruik (bijvoorbeeld over de rijstijl of de afgelegde afstand), of de technische gegevens van het voertuig (zoals gegevens over de slijtage van voertuigonderdelen), die door kruisverwijzingen met andere bestanden en met name het voertuigidentificatienummer (VIN) in verband kunnen worden gebracht met een natuurlijke persoon. Persoonsgegevens in verbonden voertuigen kunnen ook metagegevens omvatten, zoals de onderhoudsstatus van het voertuig. Met andere woorden, alle gegevens die in verband kunnen worden gebracht met een natuurlijke persoon, vallen binnen de reikwijdte van dit document.
30. Bij het kader waarin het verbonden voertuig functioneert, is een breed spectrum van belanghebbenden betrokken. Dit kader omvat zowel de traditionele actoren uit de auto-industrie als opkomende spelers uit de digitale sector. Deze richtsnoeren zijn dan ook bedoeld voor voertuigfabrikanten, fabrikanten van apparatuur en toeleveranciers van de auto-industrie, autoreparateurs, autohandelaren, aanbieders van voertuigdiensten, wagenparkbeheerders, autoverzekeringsmaatschappijen, amusementsaanbieders, telecombedrijven, beheerders van wegeninfrastructuur en overheidsinstanties, alsmede voor de betrokkenen. De EDPB onderstreept dat de categorieën betrokkenen per dienst zullen verschillen (bijvoorbeeld bestuurders, eigenaars, passagiers enz.). Dit is een niet-uitputtende lijst, aangezien het kader een grote verscheidenheid aan diensten omvat, waaronder diensten waarvoor een directe authenticatie of identificatie nodig is en diensten waarvoor dit niet nodig is.
31. Bepaalde gegevensverwerkingen die door natuurlijke personen in het voertuig worden verricht, komen neer op “de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit” en vallen als zodanig buiten het toepassingsgebied van de AVG²¹. Daarbij gaat het met name om het gebruik van persoonsgegevens binnen de voertuigen door de enige betrokkenen die deze gegevens in het dashboard van het voertuig hebben ingevoerd. De EDPB herinnert er evenwel aan dat de AVG volgens overweging 18 daarvan geldt “voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten”.

1.3.1 Wat valt buiten de reikwijdte van dit document?

32. Werkgevers die bedrijfswagens ter beschikking stellen van hun personeel, willen wellicht toezicht houden op de handelingen van hun werknemers (bijvoorbeeld om de veiligheid van de werknemer, goederen of voertuigen te waarborgen, middelen toe te wijzen, een dienst te traceren en te factureren of de arbeidstijd te controleren). De gegevensverwerking door werkgevers in deze context gaat gepaard met specifieke overwegingen inzake de

²¹ Zie artikel 2, lid 2, punt c), van de AVG.

arbeidscontext, die mogelijk geregeld zijn in nationale arbeidswetgeving die niet uitvoerig aan de orde kan komen in deze richtsnoeren²².

33. Hoewel de gegevensverwerking in het kader van voor professionele doeleinden gebruikte commerciële voertuigen (zoals openbaar vervoer) en gedeeld vervoer en oplossingen in het kader van mobiliteit als dienst (MaaS) gepaard kan gaan met specifieke overwegingen die buiten de reikwijdte van deze algemene richtsnoeren vallen, zullen veel van de hier uiteengezette beginselen en aanbevelingen ook van toepassing zijn op die vormen van verwerking.
34. Aangezien verbonden voertuigen radiografisch compatibele systemen zijn, zijn zij onderhevig aan passieve tracking, bijvoorbeeld door middel van wifi of bluetooth. In die zin verschillen zij niet van andere verbonden apparaten en vallen zij binnen het toepassingsgebied van de e-privacyrichtlijn, die momenteel wordt herzien. Het op grote schaal volgen van met wifi uitgeruste voertuigen²³ door een geconcentreerd netwerk van omstanders die gangbare smartphonelocatiediensten gebruiken, valt derhalve ook buiten de reikwijdte van dit document. Deze diensten rapporteren routinematig alle zichtbare wifinetwerken aan centrale servers. Ingebouwde wifi kan als een secundaire voertuigidentificatie²⁴ worden beschouwd en dreigt zodoende gepaard te gaan met de stelselmatige, continue verzameling van volledige voertuigbewegingsprofielen.
35. Voertuigen worden in toenemende mate uitgerust met opnameapparatuur (zoals parkeercamerasystemen en dashcams). Aangezien daarbij openbare plaatsen worden gefilmd en dat een beoordeling vereist van het desbetreffende, per lidstaat verschillende rechtskader, valt deze gegevensverwerking buiten de reikwijdte van deze richtsnoeren.
36. De verwerking van gegevens die coöperatieve intelligente vervoerssystemen (C-ITS) mogelijk maken, zoals gedefinieerd in Richtlijn 2010/40/EU²⁵, komt aan bod in een specifiek advies van de Groep gegevensbescherming artikel 29²⁶. Hoewel de definitie van C-ITS in de richtlijn geen betrekking heeft op technische specificaties, richt de Groep gegevensbescherming artikel 29 zich in zijn advies op communicatie over korte afstand, d.w.z. zonder tussenkomst van een netwerkexploitant. In het advies worden specifieke gebruiksvormen die zich in de beginfase van de uitvoering bevinden, geanalyseerd. In een later stadium zullen de nieuwe problemen worden geëvalueerd die zich ongetwijfeld zullen voordoen zodra de automatisering verder wordt uitgerold. Aangezien de gegevensbescherming zeer specifieke implicaties heeft in het kader van C-ITS (ongekende hoeveelheden locatiegegevens, voortdurende verspreiding van persoonsgegevens, uitwisseling van gegevens tussen voertuigen en andere weginfrastructuurvoorzieningen enz.) en er op Europees niveau nog over wordt gesproken, valt de verwerking van persoonsgegevens in die context niet onder deze richtsnoeren.

²² De Groep gegevensbescherming artikel 29 gaat hier nader op in in Advies 2/2017 over gegevensverwerking op het werk; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

²³ Voor meer informatie, zie: <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html>

²⁴ Markus Ullmann, Tobias Franz, en Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier - Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, Frankrijk, 23-27 juli 2017, blz. 32-37.

²⁵ Richtlijn 2010/40/EU van 7 juli 2020 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen; <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32010L0040>

²⁶ Groep gegevensbescherming artikel 29 — Advies 3/2017 over de verwerking van persoonsgegevens in het kader van coöperatieve intelligente vervoerssystemen (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

37. Tot slot wordt met dit document niet beoogd om alle mogelijke kwesties en vragen in verband met verbonden voertuigen te behandelen en kan het dus niet als een uitputtend document worden beschouwd.

1.4 Definities

38. De **verwerking** van persoonsgegevens omvat alle bewerkingen waarbij persoonsgegevens zijn betrokken, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens enz.²⁷.
39. De **betrokkene** is de natuurlijke persoon op wie de verwerkte gegevens betrekking hebben. In het kader van verbonden voertuigen is dat de bestuurder (de hoofdbestuurder of de rijder), de passagier of de eigenaar van het voertuig²⁸.
40. De **verwerkingsverantwoordelijke** is de persoon die de doeleinden en middelen voor de verwerking in verbonden voertuigen bepaalt²⁹. Verwerkingsverantwoordelijken kunnen dienstverleners zijn die voertuiggegevens verwerken om de bestuurder verkeersinformatie, berichten over zuinig rijden of waarschuwingen over de werking van het voertuig te sturen, verzekeringsmaatschappijen die verzekeringen aanbieden op basis van de afgelegde kilometers, of voertuigfabrikanten die gegevens verzamelen over de slijtage van de voertuigonderdelen om de kwaliteit ervan te verbeteren. Krachtens artikel 26 AVG kunnen twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen voor de verwerking bepalen en aldus als gezamenlijke verwerkingsverantwoordelijken worden beschouwd. In dat geval moeten zij hun respectieve verplichtingen duidelijk vaststellen, met name met betrekking tot de uitoefening van de rechten van de betrokkenen en hun respectieve verplichtingen om de in de artikelen 13 en 14 AVG bedoelde informatie te verstrekken.
41. De **verwerker** is eenieder die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt³⁰. De verwerker verzamelt en verwerkt gegevens in opdracht van de verwerkingsverantwoordelijke, zonder die gegevens voor eigen doeleinden te gebruiken. Zo kunnen fabrikanten van apparatuur en toeleveranciers van de auto-industrie in bepaalde gevallen gegevens verwerken ten behoeve van voertuigfabrikanten (wat niet betekent dat zij geen verwerkingsverantwoordelijke kunnen zijn voor andere doeleinden). Naast de verplichting voor gegevensverwerkers om passende technische en organisatorische maatregelen in te voeren om een aan het risico aangepast beveiligingsniveau te waarborgen, worden in artikel 28 AVG de verplichtingen van gegevensverwerkers uiteengezet.
42. De **ontvanger** is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt³¹. Zo is een commerciële partner van de dienstverlener die door het voertuig gegenereerde persoonsgegevens ontvangt van de dienstverlener, een ontvanger van persoonsgegevens. Ongeacht of zij optreden als nieuwe verwerkingsverantwoordelijke of als verwerker, moeten zij voldoen aan alle verplichtingen van de AVG.

²⁷ Zie artikel 4, punt 2, van de AVG.

²⁸ Zie artikel 4, punt 1, van de AVG.

²⁹ Zie artikel 4, punt 7, AVG en het Europees Comité voor gegevensbescherming, [Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#) (Richtsnoeren 7/2020 inzake de begrippen verwerkingsverantwoordelijke en verwerker in de AVG).

³⁰ Zie artikel 4, punt 8, van de AVG en Richtsnoeren 7/2020.

³¹ Zie artikel 4, punt 9, van de AVG en Richtsnoeren 7/2020.

43. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het recht van de lidstaten gelden echter niet als ontvangers³². De verwerking van die gegevens door die overheidsinstanties moet stroken met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn. Wetshandavingsinstanties zijn bijvoorbeeld geautoriseerde derden wanneer zij persoonsgegevens opvragen in het kader van een onderzoek overeenkomstig het Unierecht of het recht van de lidstaten.

1.5 Risico's met betrekking tot de persoonlijke levenssfeer en gegevensbescherming

44. De Groep gegevensbescherming artikel 29 heeft verschillende malen zorgen geuit over systemen in het kader van het internet van de dingen (Internet of Things, IoT) die ook kunnen gelden voor verbonden voertuigen³³. De reeds aangehaalde kwesties met betrekking tot de veiligheid en controle van gegevens in het kader van het internet van de dingen, liggen nog gevoeliger in de context van verbonden voertuigen, aangezien de verkeersveiligheid in het gedrang kan komen en de fysieke integriteit van de bestuurder gevaar kan lopen in een omgeving die van oudsher wordt beschouwd als geïsoleerd en beschermd tegen externe inmenging.
45. Verbonden voertuigen geven ook aanleiding tot aanzienlijke zorgen met betrekking tot gegevensbescherming en de persoonlijke levenssfeer bij de verwerking van locatiegegevens, die steeds indringender wordt en zodoende de huidige mogelijkheden om anoniem te blijven onder druk kan zetten. De EDPB wil bijzondere nadruk leggen op en belanghebbenden bewust maken van het feit dat het gebruik van locatietechnologieën de invoering van specifieke waarborgen vereist om toezicht op personen en misbruik van de gegevens te voorkomen.

1.5.1 Gebrek aan controle en een ongelijke informatiepositie

46. Voertuigbestuurders en -passagiers worden niet altijd naar behoren geïnformeerd over de verwerking van gegevens in of via een verbonden voertuig. De informatie wordt soms alleen verstrekt aan de voertuigeigenaar, die niet de bestuurder hoeft te zijn, en soms wordt de informatie niet tijdig verstrekt. Zodoende bestaat het risico dat de betrokken personen over onvoldoende functionaliteiten of opties beschikken om de controle uit te oefenen die nodig is om hun rechten inzake gegevensbescherming en de persoonlijke levenssfeer te kunnen uitoefenen. Dit punt is van belang omdat voertuigen tijdens hun levensduur aan meer dan één eigenaar kunnen toebehoren, hetzij omdat ze worden verkocht, hetzij omdat ze worden geleased in plaats van gekocht.
47. Ook kan de communicatie in het voertuig automatisch en standaard op gang worden gebracht, zonder dat de betrokkene daarvan op de hoogte is. Wanneer het niet mogelijk is om de interactie tussen het voertuig en de verbonden apparatuur doeltreffend te controleren, wordt het voor de gebruiker buitengewoon moeilijk om de gegevensstroom te beheersen. Het is in dat geval nog moeilijker om het verdere gebruik ervan te controleren en zo mogelijke functieverhuizing te voorkomen.

1.5.2 Kwaliteit van de toestemming van de gebruiker

48. De EDPB onderstreept dat indien de gegevensverwerking op toestemming berust, alle voorwaarden inzake geldige toestemming moeten worden nageleefd, wat betekent dat er sprake moet zijn van vrije, specifieke en geïnformeerde toestemming die een ondubbelzinnige wilsuiting van de betrokkene vormt, zoals uitgelegd in de EDPB-

³² Artikel 4, punt 9, en overweging 31 van de AVG.

³³ Groep gegevensbescherming artikel 29 — Advies 8/2014 over de recente ontwikkelingen op het gebied van het internet van de dingen; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_nl.pdf

richtsnoeren inzake toestemming³⁴. De verwerkingsverantwoordelijken moeten zorgvuldig omgaan met de modaliteiten voor het verkrijgen van geldige toestemming van verschillende deelnemers, zoals autobezitters en -gebruikers. Deze toestemming moet afzonderlijk en voor specifieke doeleinden worden gegeven en mag niet worden gebundeld met de koop- of leasingovereenkomst voor een nieuwe auto. De toestemming moet even gemakkelijk kunnen worden ingetrokken als zij is gegeven.

49. Hetzelfde geldt wanneer toestemming vereist is om aan de e-privacyrichtlijn te voldoen, bijvoorbeeld wanneer informatie wordt opgeslagen of toegang wordt verleend tot informatie die reeds in het voertuig is opgeslagen, zoals in bepaalde gevallen vereist krachtens artikel 5, lid 3, van de e-privacyrichtlijn. Zoals hierboven uiteengezet, moet toestemming in deze context immers worden geïnterpreteerd in het licht van de AVG.
50. In veel gevallen is de gebruiker zich niet bewust van de gegevensverwerking die in zijn/haar voertuig plaatsvindt. Een dergelijk gebrek aan informatie vormt een aanzienlijke belemmering om aan te tonen dat geldige toestemming is verkregen in het kader van de AVG, aangezien de toestemming geïnformeerd moet zijn. In dergelijke omstandigheden kan toestemming niet worden ingeroepen als rechtsgrond voor de overeenkomstige gegevensverwerking uit hoofde van de AVG.
51. Klassieke mechanismen die worden gebruikt om de toestemming van natuurlijke personen te verkrijgen, zijn mogelijk moeilijk toepasbaar in het kader van verbonden voertuigen en kunnen resulteren in toestemming van “lage kwaliteit” op basis van een gebrek aan informatie of in de feitelijke onmogelijkheid om de toestemming nauwkeurig af te stemmen op de door natuurlijke personen kenbaar gemaakte voorkeuren. In de praktijk kan het ook moeilijk zijn toestemming te krijgen van bestuurders en passagiers die niet verwant zijn aan de eigenaar van het voertuig in het geval van tweedehands, geleasede, gehuurde of geleende voertuigen.
52. Wanneer de e-privacyrichtlijn geen toestemming van de betrokkene vereist, is de verwerkingsverantwoordelijke niettemin verantwoordelijk voor het kiezen van de rechtsgrond krachtens artikel 6 AVG die in het specifieke geval het meest geschikt is voor de verwerking van persoonsgegevens.

1.5.3 Verdere verwerking van persoonsgegevens

53. Wanneer gegevens worden verzameld op basis van toestemming zoals vereist door artikel 5, lid 3, van de e-privacyrichtlijn of op grond van een van de uitzonderingen van artikel 5, lid 3, en vervolgens worden verwerkt overeenkomstig artikel 6 AVG, mogen zij alleen verder worden verwerkt indien de verwerkingsverantwoordelijke aanvullende toestemming vraagt voor dit andere doel of indien hij/zij kan aantonen dat de toestemming is gebaseerd op bepalingen van het Unierecht of het recht van de lidstaten bepalingen ter waarborging van de doelstellingen als bedoeld in artikel 23, lid 1, van de AVG³⁵. De EDPB is van mening dat verdere verwerking op basis van een verenigbaarheidstoets overeenkomstig artikel 6, lid 4, van de AVG in dergelijke gevallen niet mogelijk is, aangezien dit de gegevensbeschermingsnorm van de e-privacyrichtlijn zou ondermijnen. Wanneer de e-privacyrichtlijn toestemming vereist, moet die immers specifiek en geïnformeerd zijn, wat betekent dat de betrokkenen op de hoogte moeten zijn van alle doeleinden van de gegevensverwerking en het recht hebben specifieke doeleinden te weigeren³⁶. Wanneer verdere verwerking op basis van een verenigbaarheidstoets overeenkomstig artikel 6, lid 4,

³⁴ Europees Comité voor gegevensbescherming, [Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679](#), versie 1.1, 4 mei 2020.

³⁵ Zie ook Europees Comité voor gegevensbescherming, [Guidelines 10/2020 on restrictions under Article 23 GDPR](#) (Richtsnoeren 10/2020 inzake beperkingen uit hoofde van artikel 23 AVG).

³⁶ Richtsnoeren 05/2020, punten 3.2 en 3.3.

van de AVG wordt beschouwd als een mogelijkheid, wordt het beginsel van de in de huidige richtlijn neergelegde toestemmingsvereisten omzeild.

54. De EDPB herinnert eraan dat de aanvankelijke toestemming nooit een legitimatie vormt voor verdere verwerking, aangezien toestemming alleen geldig is als zij geïnformeerd en specifiek is.
55. Zo mogen telemetriegegevens die tijdens het gebruik van het voertuig voor onderhoudsdoeleinden worden verzameld, niet zonder toestemming van de gebruiker aan autoverzekeringsmaatschappijen worden meegedeeld met het oog op het opstellen van bestuurdersprofielen om op het rijgedrag gebaseerde verzekeringspolissen aan te bieden.
56. Voorts kunnen door verbonden voertuigen verzamelde gegevens door wetshandhavingsinstanties worden verwerkt om snelheidsovertredingen of andere overtredingen op te sporen, voor zover en wanneer aan de specifieke voorwaarden van de richtlijn wetshandhaving is voldaan. In dat geval worden dergelijke gegevens beschouwd als betrekking hebbend op strafrechtelijke veroordelingen en strafbare feiten onder de voorwaarden die zijn neergelegd in artikel 10 AVG en de toepasselijke nationale wetgeving. Fabrikanten mogen dergelijke gegevens aan de wetshandhavingsinstanties verstrekken indien aan de specifieke voorwaarden voor een dergelijke verwerking is voldaan. De EDPB wijst erop dat de verwerking van persoonsgegevens met als enig doel te voldoen aan verzoeken van wetshandhavingsinstanties geen welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde is in de zin van artikel 5, lid 1, punt b), van de AVG. Wanneer wetshandhavingsinstanties daartoe bij wet gemachtigd zijn, kunnen zij derden zijn in de zin van artikel 4, punt 10, van de AVG. In dat geval zijn fabrikanten gerechtigd die instanties alle gegevens te verstrekken waarover zij beschikken, mits het desbetreffende rechtskader in elke lidstaat wordt nageleefd.

1.5.4 Buitensporige gegevensverzameling

57. Nu er steeds meer sensoren worden ingebouwd in verbonden voertuigen, bestaat er een zeer groot risico dat er meer gegevens worden verzameld dan nodig is om het doel te bereiken.
58. Voor de ontwikkeling van nieuwe functionaliteiten, en in het bijzonder functionaliteiten die gebaseerd zijn op machinaal lerende algoritmen, kan een grote hoeveelheid gegevens nodig zijn die over een lange periode worden verzameld.

1.5.5 Persoonsgegevensbeveiliging

59. Door het grote aantal functionaliteiten, diensten en interfaces (bijvoorbeeld web, USB, RFID, wifi) van verbonden voertuigen wordt het doelwit vergroot en zodoende ook het aantal potentiële zwakke plekken waardoor persoonsgegevens in gevaar kunnen worden gebracht. In tegenstelling tot de meeste IoT-apparaten (internet of things), zijn verbonden voertuigen kritieke systemen waarbij een inbreuk op de beveiliging het leven van de gebruikers en de omstanders in gevaar kan brengen. Het is dus van het allergrootste belang het risico aan te pakken dat hackers de kwetsbaarheden van verbonden voertuigen trachten uit te buiten.
60. Bovendien moeten persoonsgegevens die in voertuigen en/of op externe locaties (bijvoorbeeld in cloud computing-infrastructuren) zijn opgeslagen, afdoende worden beveiligd tegen ongeoorloofde toegang. Zo moet een voertuig voor een onderhoudsbeurt worden toevertrouwd aan een monteur, die toegang moet krijgen tot bepaalde technische voertuiggegevens. Hoewel de monteur toegang moet hebben tot de technische gegevens, bestaat de mogelijkheid dat hij/zij toegang probeert te krijgen tot alle in het voertuig opgeslagen gegevens.

61. Om de hierboven beschreven risico's voor de betrokkenen te beperken, moeten de volgende algemene aanbevelingen in acht worden genomen door fabrikanten van voertuigen en van apparatuur, dienstverleners en alle andere belanghebbenden die kunnen optreden als verwerkingsverantwoordelijke of verwerker van gegevens in het kader van verbonden voertuigen.

2.1 Categorieën gegevens

62. Zoals in de inleiding is opgemerkt, worden de meeste gegevens in verband met verbonden voertuigen beschouwd als persoonsgegevens, voor zover zij in verband kunnen worden gebracht met een of meer identificeerbare natuurlijke personen. Technische gegevens over de bewegingen van het voertuig (zoals de snelheid en de afgelegde afstand) en over de toestand van het voertuig (bijvoorbeeld de temperatuur van de motorkoelvloeistof, het motortoerental, de bandenspanning) vallen hier ook onder. Bepaalde gegevens die door verbonden voertuigen worden gegenereerd, kunnen ook bijzondere aandacht verdienen gezien hun gevoeligheid en/of potentiële impact op de rechten en belangen van de betrokkenen. Momenteel heeft de EDPB drie categorieën van persoonsgegevens geïdentificeerd waar fabrikanten van voertuigen en van apparatuur, dienstverleners en andere verwerkingsverantwoordelijken bijzondere aandacht aan moeten besteden: locatiegegevens, biometrische gegevens (en alle in artikel 9 AVG omschreven speciale gegevenscategorieën) en gegevens die strafbare feiten of verkeersovertredingen aan het licht zouden kunnen brengen.

2.1.1 Locatiegegevens

63. Bij het verzamelen van persoonsgegevens moeten fabrikanten van voertuigen en apparatuur, van dienstverleners en andere verwerkingsverantwoordelijken voor ogen houden dat locatiegegevens bijzonder veel inzicht bieden in de leefgewoonten van de betrokkenen. De afgelegde ritten zijn zeer kenmerkend, omdat daaruit kan worden afgeleid waar de bestuurder werkt en woont en wat zijn/haar interesses zijn (vrijtijdsbesteding), en omdat daaruit mogelijk gevoelige informatie naar voren kan komen, bijvoorbeeld over godsdienst via de plaats van eredienst, of seksuele geaardheid via de bezochte plaatsen. De fabrikant van het voertuig en van de apparatuur, de dienstverlener en andere verwerkingsverantwoordelijken moeten er dan ook bijzonder goed op letten geen locatiegegevens te verzamelen, tenzij dat absoluut noodzakelijk is voor het doel van de verwerking. Wanneer de verwerking bijvoorbeeld bestaat in het detecteren van de beweging van het voertuig, volstaat de gyroscoop om die functie te vervullen en is het niet nodig om locatiegegevens te verzamelen.

64. In het algemeen moet ook het verzamelen van locatiegegevens voldoen aan de volgende beginselen:

- Z Er moeten een passende frequentie van de toegang tot de verzamelde locatiegegevens en een passende mate van gedetailleerdheid daarvan worden vastgesteld die in verhouding staan tot het doel van de verwerking. Een weertoepassing mag bijvoorbeeld niet elke seconde toegang hebben tot de locatie van het voertuig, zelfs niet met toestemming van de betrokkene.
- Z Er moet nauwkeurige informatie worden verstrekt over het doel van de verwerking (bijvoorbeeld: wordt de locatiegeschiedenis opgeslagen? Zo ja, waarom?).
- Z Wanneer de verwerking op toestemming is gebaseerd, moet geldige (vrije, specifieke en geïnformeerde) toestemming worden verkregen die losstaat van de algemene verkoop- of gebruiksvoorwaarden, bijvoorbeeld op de boordcomputer.

- Z De locatie mag alleen worden ingeschakeld wanneer de gebruiker een functie start waarvoor de locatie van het voertuig bekend moet zijn, en mag niet standaard en continu worden ingeschakeld bij het starten van de auto.
- Z De gebruiker moet ervan op de hoogte worden gesteld dat de locatie is geactiveerd, met name door middel van pictogrammen (bijvoorbeeld een pijl die over het scherm beweegt).
- Z Het moet mogelijk zijn de locatie op elk moment uit te schakelen.
- Z Er moet een beperkte opslagperiode worden vastgesteld.

2.1.2 Biometrische gegevens

65. In het kader van verbonden voertuigen kunnen biometrische gegevens worden verwerkt die worden gebruikt met het oog op de unieke identificatie van een persoon, binnen de werkingssfeer van artikel 9 AVG en de nationale uitzonderingen, onder meer om toegang tot een voertuig mogelijk te maken, om de bestuurder/eigenaar te authenticeren en/of om toegang te krijgen tot de profielinstellingen en -voorkeuren van een bestuurder. Wanneer het gebruik van biometrische gegevens wordt overwogen, houdt het garanderen van volledige controle van de betrokkene over zijn of haar gegevens in dat er enerzijds een niet-biometrisch alternatief beschikbaar wordt gesteld (bijvoorbeeld het gebruik van een fysieke sleutel of een code) zonder extra beperkingen (het gebruik van biometrische gegevens mag dus niet verplicht zijn), en dat anderzijds het biometrische sjabloon uitsluitend lokaal in gecodeerde vorm wordt opgeslagen en vergeleken, waarbij de biometrische gegevens niet worden verwerkt door een externe uitlees- of vergelijkingsterminal.

66. In het geval van biometrische gegevens³⁷ is het van belang ervoor te zorgen dat de biometrische authenticatieoplossing voldoende betrouwbaar is, met name door de volgende beginselen in acht te nemen:

- Z De aanpassing van de gebruikte biometrische oplossing (bijvoorbeeld het percentage foutpositieven en fout-negatieven) is afgestemd op het beveiligingsniveau van de vereiste toegangscontrole.
- Z De gebruikte biometrische oplossing is gebaseerd op een sensor die bestand is tegen aanvallen (zoals het gebruik van een vlakke afdruk voor vingerafdrukherkenning).
- Z Het aantal authenticatiepogingen is beperkt.
- Z Het biometrische sjabloon/model wordt in het voertuig opgeslagen, in gecodeerde vorm met gebruikmaking van een cryptografisch algoritme en sleutelbeheer die in overeenstemming zijn met de laatste technologische ontwikkelingen.
- Z De ruwe gegevens die worden gebruikt om het biometrische sjabloon op te maken en voor de authenticatie van de gebruiker, worden in realtime verwerkt zonder ooit te worden opgeslagen, ook niet lokaal.

2.1.3 Gegevens waaruit strafbare feiten of andere overtredingen blijken

67. Voor de verwerking van gegevens die betrekking hebben op mogelijke strafbare feiten in de zin van artikel 10 AVG, beveelt de EDPB aan de gegevens lokaal te verwerken waarbij de betrokkene de volledige controle heeft over de verwerking (zie de bespreking van lokale verwerking in punt 2.4). Op enkele uitzonderingen na (zie de casestudy over de bestudering van de oorzaken en gevolgen van ongevallen in punt 3.3) is externe verwerking van gegevens die strafbare feiten of andere overtredingen aan het licht brengen, verboden. Afhankelijk van de gevoeligheid van de gegevens moeten derhalve sterke beveiligingsmaatregelen

³⁷ De verbodsbepaling van artikel 9, lid 1, AVG heeft uitsluitend betrekking op “biometrische gegevens met het oog op de unieke identificatie van een persoon”.

worden getroffen, zoals de in punt 2.7 beschreven maatregelen, om bescherming te bieden tegen onrechtmatige toegang tot, wijziging of verwijdering van die gegevens.

68. Bepaalde categorieën van persoonsgegevens van verbonden voertuigen kunnen immers aan het licht brengen dat er een strafbaar feit of een andere overtreding is of wordt begaan (“overtredingsgerelateerde gegevens”) en kunnen daarom aan bijzondere beperkingen onderworpen zijn (bijvoorbeeld gegevens die aangeven dat het voertuig een witte lijn heeft overschreden, de momentane snelheid van een voertuig in combinatie met precieze locatiegegevens). Met name wanneer dergelijke gegevens door de bevoegde nationale autoriteiten worden verwerkt met het oog op strafrechtelijk onderzoek en de vervolging van strafbare feiten, zijn de waarborgen van artikel 10 AVG van toepassing.

2.2 Doeleinden

69. Persoonsgegevens mogen worden verwerkt voor een breed scala van doeleinden met betrekking tot verbonden voertuigen, waaronder de veiligheid van de bestuurder, verzekering, efficiënt vervoer, entertainment of informatiediensten. In overeenstemming met de AVG moeten de verwerkingsverantwoordelijken ervoor zorgen dat hun doeleinden “welbepaald, uitdrukkelijk en gerechtvaardigd” zijn, dat de persoonsgegevens vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt en dat er een geldige rechtsgrond is voor de verwerking, zoals vereist bij artikel 5 AVG. In deel III van deze richtsnoeren komen enkele concrete voorbeelden aan bod van mogelijke doeleinden van verwerkingsverantwoordelijken die actief zijn op het gebied van verbonden voertuigen en worden specifieke aanbevelingen gedaan voor elk type verwerking.

2.3 Relevantie en minimale gegevensverwerking

70. Om te voldoen aan het beginsel van minimale gegevensverwerking³⁸, moeten fabrikanten van voertuigen en van apparatuur, dienstverleners en andere verwerkingsverantwoordelijken speciale aandacht besteden aan de categorieën van gegevens die zij van een verbonden voertuig nodig hebben, aangezien zij alleen persoonsgegevens mogen verzamelen die relevant en noodzakelijk zijn voor de verwerking. Locatiegegevens zijn namelijk bijzonder indringend en kunnen veel inzicht bieden in de leefgewoonten van de betrokkenen. Deelnemers uit de sector moeten dan er dan ook bijzonder op letten geen locatiegegevens te verzamelen, tenzij dat absoluut noodzakelijk is voor het verwerkingsdoeleinde (zie de bespreking van locatiegegevens hierboven in punt 2.1).

³⁸ Artikel 5, lid 1, punt c), van de AVG.

2.4 Gegevensbescherming door ontwerp en door standaardinstellingen

71. Gelet op het volume en de diversiteit van de door verbonden voertuigen geproduceerde persoonsgegevens, merkt de EDPB op dat de verwerkingsverantwoordelijken ervoor moeten zorgen dat in het kader van verbonden voertuigen gebruikte technologieën zodanig zijn afgesteld dat de persoonlijke levenssfeer van natuurlijke personen wordt geëerbiedigd door de verplichtingen inzake gegevensbescherming door ontwerp en door standaardinstellingen toe te passen, zoals vereist bij artikel 25 AVG. De technologieën moeten zodanig zijn ontworpen dat de verzameling van persoonsgegevens tot een minimum wordt beperkt, moeten standaardinstellingen hebben die de persoonlijke levenssfeer beschermen en ervoor zorgen dat de betrokkenen goed worden geïnformeerd en de mogelijkheid hebben om configuraties in verband met hun persoonsgegevens gemakkelijk te wijzigen. Specifieke richtsnoeren over de wijze waarop fabrikanten en dienstverleners kunnen voldoen aan gegevensbescherming door ontwerp en door standaardinstellingen kunnen nuttig zijn voor de sector en voor derden die toepassingen aanbieden.
72. Bepaalde algemene praktijken, die hieronder worden beschreven, kunnen ook helpen om de risico's voor de rechten en vrijheden van natuurlijke personen in verband met verbonden voertuigen, te beperken³⁹.

2.4.1 Lokale verwerking van persoonsgegevens

73. In algemene zin moeten fabrikanten van voertuigen en van apparatuur, dienstverleners en andere verwerkingsverantwoordelijken waar mogelijk processen hanteren waarbij geen persoonsgegevens worden gebruikt en geen persoonsgegevens worden doorgegeven buiten het voertuig (d.w.z. dat de gegevens in het voertuig worden verwerkt). De aard van verbonden voertuigen brengt echter risico's met zich mee, zoals de mogelijkheid van aanvallen op de lokale verwerking door externe actoren of het lekken van lokale gegevens als gevolg van de verkoop van voertuigonderdelen. Daarom moet de nodige aandacht worden besteed aan en moeten beveiligingsmaatregelen worden getroffen om ervoor te zorgen dat lokale verwerking lokaal blijft. Dit scenario biedt het voordeel dat de gebruiker de uitsluitende en volledige controle over zijn/haar persoonsgegevens heeft, waardoor het "door ontwerp" minder risico's voor de persoonlijke levenssfeer inhoudt, met name omdat elke verwerking van gegevens door belanghebbenden zonder medeweten van de betrokkene verboden is. Het scenario maakt ook de verwerking van gevoelige gegevens mogelijk, zoals biometrische gegevens of gegevens in verband met strafbare feiten of andere overtredingen, alsook gedetailleerde locatiegegevens, die anders aan strengere regels onderworpen zouden zijn (zie hieronder). In dezelfde geest brengt dit scenario minder cyberbeveiligingsrisico's en weinig vertraging met zich mee, waardoor het bijzonder geschikt is voor geautomatiseerde rijassistentie. Enkele voorbeelden van dit type oplossing zijn:
- Z toepassingen voor zuinig rijden die gegevens in het voertuig verwerken om in realtime adviezen over zuinig rijden weer te geven op het scherm aan boord;
 - Z toepassingen waarbij persoonsgegevens worden doorgegeven aan een apparaat zoals een smartphone dat volledig onder controle staat van de gebruiker (bijvoorbeeld via bluetooth of wifi) en waarbij de voertuiggegevens niet worden doorgezonden naar de aanbieders van de toepassing of de voertuigfabrikanten; dit omvat bijvoorbeeld de koppeling van smartphones om het beeldscherm, de multimediasystemen, de microfoon (of andere sensoren) van de auto te gebruiken voor telefoongesprekken enz., voor zover de verzamelde gegevens onder de

³⁹ Zie ook Europees Comité voor gegevensbescherming, [Richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen](#), versie 2.0, aangenomen op 20 oktober 2020.

controle van de betrokkene blijven en uitsluitend worden gebruikt om de dienst te verlenen waarom hij of zij heeft verzocht;

- Z toepassingen die de veiligheid in het voertuig verhogen, zoals toepassingen die geluidssignalen geven of het stuur doen trillen wanneer een bestuurder een auto inhaalt zonder de richting aan te geven of over de witte lijn rijdt, of die waarschuwingen geven over de toestand van het voertuig (bijvoorbeeld over slijtage van de remblokken);
 - Z toepassingen om bepaalde voertuigcommando's te ontgrendelen, te starten en/of te activeren met behulp van de in het voertuig opgeslagen biometrische gegevens van de bestuurder (zoals een gezichts- of stemmodel of de specifieke elementen van vingerafdrukken).
74. Bij toepassingen zoals de bovengenoemde worden gegevens verwerkt voor het verrichten van zuiver persoonlijke activiteiten door een natuurlijke persoon (d.w.z. zonder dat persoonsgegevens worden doorgegeven aan een verwerkingsverantwoordelijke of een verwerker). **Daarom vallen deze toepassingen overeenkomstig artikel 2, lid 2, AVG, buiten het toepassingsgebied van de AVG.**
75. Indien de AVG niet van toepassing is op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit, geldt zij echter wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten (autofabrikanten, dienstverleners enz.), overeenkomstig overweging 18 van de AVG. Wanneer zij optreden als verwerkingsverantwoordelijke of verwerker, moeten zij dus veilige toepassingen aan boord ontwikkelen, met inachtneming van het beginsel van privacy door ontwerp en door standaardinstellingen. In elk geval geldt het volgende overeenkomstig overweging 78 van de AVG: "Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen de producenten van de producten, diensten en toepassingen te worden gestimuleerd om bij de ontwikkeling en de uitwerking van dergelijke producten, diensten en toepassingen rekening te houden met het recht op bescherming van persoonsgegevens en, met inachtneming van de stand van de techniek, erop toe te zien dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming"⁴⁰. Enerzijds zal dit de ontwikkeling van gebruikersgerichte diensten ten goede komen en anderzijds zal dit elk verder gebruik in de toekomst dat binnen het toepassingsgebied van de AVG zou kunnen vallen, vergemakkelijken en beveiligen. Meer specifiek beveelt de EDPB aan een veilig platform voor toepassingen aan boord te ontwikkelen, dat fysiek gescheiden is van de veiligheidsrelevante functies van auto's, zodat de toegang tot autogegevens niet afhankelijk is van onnodige externe cloudcapaciteit.
76. Waar mogelijk moeten autofabrikanten en dienstverleners lokale gegevensverwerking overwegen om de potentiële risico's van verwerking in de cloud te beperken, zoals wordt onderstreept in het advies van de Groep gegevensbescherming artikel 29 over cloud computing⁴¹.
77. In algemene zin moeten gebruikers zeggenschap hebben over de wijze waarop hun gegevens in het voertuig worden verzameld en verwerkt:

⁴⁰ Zie voor meer aanbevelingen over privacy door ontwerp en door standaardinstellingen ook Richtsnoeren 4/2019.

⁴¹ Groep gegevensbescherming artikel 29 — Advies 05/2012 over cloud computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_nl.pdf

- Z Informatie over de verwerking moet in de taal van de bestuurder worden verstrekt (handleiding, instellingen enz.).
 - Z De EDPB beveelt aan standaard alleen gegevens te verwerken die strikt noodzakelijk zijn voor de werking van het voertuig. De betrokkenen moeten de mogelijkheid hebben de gegevensverwerking voor elk ander doeleinde en voor elke andere verwerkingsverantwoordelijke/verwerker te activeren of te deactiveren en om de betrokken gegevens te wissen, rekening houdend met het doeleinde en de rechtsgrond van de gegevensverwerking.
 - Z De gegevens mogen niet naar derden worden doorgezonden (d.w.z. dat de gebruiker als enige toegang heeft tot de gegevens).
 - Z De gegevens mogen niet langer worden bewaard dan nodig is voor het verlenen van de dienst of anderszins door het Unierecht of het recht van de lidstaten wordt voorgeschreven.
 - Z De betrokkenen moeten de mogelijkheid hebben persoonsgegevens permanent te wissen voordat de voertuigen te koop worden aangeboden.
 - Z De betrokkenen moeten, voor zover haalbaar, rechtstreeks toegang hebben tot de gegevens die door deze toepassingen worden gegenereerd.
78. Tot slot kan, aangezien lokale gegevensverwerking niet altijd mogelijk zal zijn voor ieder gebruik, in veel gevallen worden gekozen voor “hybride verwerking”. Zo kunnen in het kader van op gebruik gebaseerde verzekeringen persoonsgegevens over het rijgedrag (zoals de kracht waarmee het rempedaal wordt ingedrukt, het aantal afgelegde kilometers enz.) ofwel in het voertuig worden verwerkt, ofwel door de telematicadienstverlener namens de verzekeringsmaatschappij (de verwerkingsverantwoordelijke) om numerieke scores te genereren die volgens een vastgestelde regeling (bijvoorbeeld maandelijks) worden doorgegeven aan de verzekeringsmaatschappij. Op die manier krijgt de verzekeringsmaatschappij geen toegang tot de ruwe gedragsgegevens, maar alleen tot de geaggregeerde score die het resultaat is van de verwerking. Dit zorgt ervoor dat door het ontwerp wordt voldaan aan de beginselen van minimale gegevensverwerking Dit betekent ook dat gebruikers hun recht moeten kunnen uitoefenen wanneer gegevens door andere partijen worden opgeslagen: een gebruiker moet bijvoorbeeld de mogelijkheid hebben om gegevens die zijn opgeslagen in de systemen van een auto-onderhoudsbedrijf of -dealer te wissen onder de voorwaarden van artikel 17 AVG.

2.4.2 Anonimisering en pseudonimisering

79. Indien het de bedoeling is dat gegevens buiten het voertuig worden doorgezonden, moet worden overwogen deze gegevens vóór doorzending te anonimiseren. Bij het anonimiseren moet de verwerkingsverantwoordelijke rekening houden met alle betrokken verwerkingen die mogelijk kunnen leiden tot heridentificatie van gegevens, zoals de doorgifte van lokaal geanonimiseerde gegevens. De EDPB herinnert eraan dat de gegevensbeschermingsbeginselen niet van toepassing zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is⁴². Zodra een gegevensreeks echt is geanonimiseerd en natuurlijke personen niet langer identificeerbaar zijn, is de Europese wetgeving inzake gegevensbescherming niet langer van toepassing. Bijgevolg kan anonimisering in voorkomend geval een goede strategie zijn om de voordelen van verbonden voertuigen te behouden en de risico's die daarmee gepaard gaan te beperken.
80. Zoals aangegeven in het advies van de Groep gegevensbescherming artikel 29 over anonimiseringstechnieken, kunnen er verschillende methoden worden gebruikt en soms gecombineerd om gegevens te anonimiseren⁴³.
81. Andere technieken, zoals pseudonimisering⁴⁴, kunnen helpen de risico's van de gegevensverwerking tot een minimum te beperken, rekening houdend met het feit dat voor de verwezenlijking van het verwerkingsdoel in de meeste gevallen geen direct identificeerbare gegevens niet nodig zijn. Indien pseudonimisering wordt versterkt met veiligheidswaarborgen, komt dat de bescherming van persoonsgegevens ten goede doordat de risico's van misbruik worden verminderd. Pseudonimisering is omkeerbaar, in tegenstelling tot anonimisering, en gepseudonimiseerde gegevens worden beschouwd als persoonsgegevens waarop de AVG van toepassing is.

2.4.3 Effectbeoordeling met betrekking tot de gegevensbescherming

82. Gezien de schaal en gevoeligheid van de persoonsgegevens die via verbonden voertuigen kunnen worden gegenereerd, zal verwerking — met name in situaties waarin persoonsgegevens buiten het voertuig worden verwerkt — vaak een hoog risico opleveren voor de rechten en vrijheden van natuurlijke personen. Waar dit het geval is, zullen de deelnemers uit de sector een gegevensbeschermingseffectbeoordeling moeten uitvoeren om de risico's te identificeren en te beperken, zoals omschreven in de artikelen 35 en 36 AVG. Zelfs indien er geen gegevensbeschermingseffectbeoordeling vereist is, is het een goede praktijk om zo vroeg mogelijk in het ontwerpproces een dergelijke beoordeling te verrichten. De deelnemers uit de sector kunnen in dat geval de resultaten van die analyse in aanmerking nemen bij hun ontwerpkeuzen voordat nieuwe technologieën worden uitgerold.

⁴² Zie artikel 4, punt 1, en overweging 26 van de AVG.

⁴³ Groep gegevensbescherming artikel 29 — Advies 5/2014 over anonimiseringstechnieken; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf

⁴⁴ Artikel 4, punt 5, van de AVG. Enisa-verslag van 3 december 2019: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>

83. Voorafgaand aan de verwerking van persoonsgegevens moet de betrokkene op de hoogte worden gebracht van de identiteit van de verwerkingsverantwoordelijke (bijvoorbeeld de fabrikanten van het voertuig en van de apparatuur of de dienstverlener), het doeleinde van de verwerking, de ontvangers van de gegevens, de periode gedurende welke de gegevens zullen worden bewaard en de rechten van de betrokkene uit hoofde van de AVG⁴⁵.

84. De fabrikanten van het voertuig en van de apparatuur, dienstverleners en andere verwerkingsverantwoordelijken moeten de betrokkene ook de volgende informatie verstrekken op een heldere, eenvoudige en makkelijk toegankelijke manier:

- Z de contactgegevens van de functionaris voor gegevensbescherming;
- Z de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;
- Z de uitdrukkelijke vermelding van de gerechtvaardigde belangen die de verwerkingsverantwoordelijke of een derde nastreeft, wanneer die gerechtvaardigde belangen de rechtsgrond voor de verwerking vormen;
- Z in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- Z de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- Z dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem/haar betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
- Z het recht de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
- Z in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie, en de waarborgen die worden gebruikt bij de doorgifte ervan;
- Z of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- Z het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering waaraan voor de betrokkene rechtsgevolgen zijn verbonden of die hem/haar in aanmerkelijke mate treft, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Dit kan met name het geval zijn bij het aanbieden van op gebruik gebaseerde verzekeringen aan natuurlijke personen;
- Z dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;
- Z informatie over verdere verwerking;
- Z in geval van gezamenlijke verwerkingsverantwoordelijken, duidelijke en volledige informatie over de verantwoordelijkheden van iedere verwerkingsverantwoordelijke.

⁴⁵ Artikel 5, lid 1, punt a), en artikel 13 van de AVG. Zie ook Groep gegevensbescherming artikel 29, [Guidelines on Transparency under Regulation 2016/679](#) (wp260rev.01), bekrachtigd door de EDPB.

85. In sommige gevallen worden persoonsgegevens niet rechtstreeks bij de betrokkene verzameld. Een fabrikant van voertuigen en van apparatuur kan bijvoorbeeld afhankelijk zijn van een dealer voor de verzameling van informatie over de voertuigeigenaar om een pechhulpdienst aan te bieden. Wanneer de gegevens niet rechtstreeks zijn verzameld, vermelden de fabrikanten van het voertuig en van de apparatuur, de dienstverlener of een andere verwerkingsverantwoordelijke naast de bovengenoemde informatie ook de betrokken categorieën van persoonsgegevens, de bron van de persoonsgegevens, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen. De verwerkingsverantwoordelijke moet die informatie binnen een redelijke termijn na het verkrijgen van de gegevens verstrekken, en **uiterlijk op de eerste van de volgende datums** overeenkomstig artikel 14, lid 3, AVG: i) binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt, ii) uiterlijk op het moment van het eerste contact met de betrokkene, of iii) indien de gegevens worden doorgezonden naar een derde, vóór de doorzending van de gegevens.
86. Mogelijk moet ook nieuwe informatie aan de betrokkenen worden verstrekt wanneer zij te maken krijgen met een nieuwe verwerkingsverantwoordelijke. Een pechhulpdienst die in verbinding staat met verbonden voertuigen kan door verschillende verwerkingsverantwoordelijken van gegevens worden voorzien, afhankelijk van het land of de regio waar de bijstand nodig is. Nieuwe verwerkingsverantwoordelijken moeten de betrokkenen de vereiste informatie verstrekken wanneer de betrokkenen een grens passeren en de diensten die interageren met de verbonden voertuigen worden overgenomen door nieuwe verwerkingsverantwoordelijken.
87. De informatie voor de betrokkenen kan op verschillende niveaus worden verstrekt⁴⁶, d.w.z. door twee informatieniveaus van elkaar te scheiden: enerzijds informatie van het eerste niveau, die het belangrijkste is voor de betrokkenen, en anderzijds informatie die vermoedelijk in een later stadium van belang is. De essentiële informatie van het eerste niveau omvat naast de identiteit van de verwerkingsverantwoordelijke ook het doelinde van de verwerking en een beschrijving van de rechten van de betrokkene, alsook alle aanvullende informatie over de verwerking die de meeste gevolgen heeft voor de betrokkene en over verwerkingen die hem/haar zou kunnen verrassen. De EDPB beveelt aan dat de betrokkene in het kader van verbonden voertuigen op de hoogte wordt gesteld van alle ontvangers op het eerste informatieniveau. Zoals opgemerkt in de richtsnoeren van de Groep gegevensbescherming artikel 29 inzake transparantie, moeten verwerkingsverantwoordelijken informatie over de ontvangers verstrekken die voor de betrokkenen het meest betekenisvol is. In de praktijk zullen dit meestal de met naam genoemde ontvangers zijn, zodat de betrokkenen precies weten welke ontvangers over hun persoonsgegevens beschikken. Indien de verwerkingsverantwoordelijken de namen van de ontvangers niet kunnen verstrekken, moet de informatie zo specifiek mogelijk zijn door het type ontvanger te vermelden (d.w.z. door te verwijzen naar de activiteiten die de ontvangers verrichten), de bedrijfstak, de sector en de subsector, en de locatie van de ontvangers.
88. De betrokkenen kunnen worden geïnformeerd door middel van beknopte en eenvoudig te begrijpen clausules in de verkoopovereenkomst van het voertuig, in de dienstverleningsovereenkomst en/of op een willekeurige schriftelijke drager, door afzonderlijke documenten (bijvoorbeeld het onderhoudsboekje of de handleiding van het voertuig) of de boordcomputer te gebruiken.
89. Er kunnen gestandaardiseerde pictogrammen worden gebruikt in aanvulling op de informatie die is vereist krachtens de artikelen 13 en 14 AVG, om de transparantie te

⁴⁶ Zie ook Groep gegevensbescherming artikel 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679 (wp260rev.01), bekrachtigd door de EDPB.

vergroten door mogelijk te voorkomen dat grote hoeveelheden schriftelijke informatie aan een betrokkene moeten worden verstrekt. De informatie moet zichtbaar zijn in voertuigen om een goed, begrijpelijk en duidelijk leesbaar overzicht te bieden van de voorgenomen verwerking. De EDPB benadrukt het belang om die pictogrammen te standaardiseren, zodat de gebruiker dezelfde symbolen aantreft ongeacht het merk of model van het voertuig. Zo kan een duidelijk signaal aan boord worden afgegeven (bijvoorbeeld een lampje in het voertuig) om de passagiers ervan op de hoogte te stellen dat bepaalde gegevens worden verzameld, zoals locatiegegevens.

2.6 Rechten van de betrokkene

90. Fabrikanten van voertuigen en van apparatuur, dienstverleners en andere verwerkingsverantwoordelijken moeten het de betrokkenen gemakkelijker maken om gedurende de gehele verwerkingsperiode controle over hun gegevens uit te oefenen, door middel van specifieke instrumenten waarmee zij hun rechten doeltreffend kunnen uitoefenen, met name hun recht van inzage, rectificatie, wissing, beperking van de verwerking en, afhankelijk van de rechtsgrond van de verwerking, hun recht op overdraagbaarheid van gegevens en hun recht van bezwaar.
91. Om het wijzigen van de instellingen te vergemakkelijken, moet een profielbeheersysteem worden gebruikt om de voorkeuren van bekende bestuurders op te slaan en hen te helpen hun privacyinstellingen op elk moment gemakkelijk te wijzigen. Het profielbeheersysteem moet alle gegevensinstellingen voor elke gegevensverwerking centraliseren, met name om de toegang tot en de wissing, verwijdering en overdraagbaarheid van persoonsgegevens uit voertuigsystemen op verzoek van de betrokkene te vergemakkelijken. Bestuurders moeten de mogelijkheid krijgen de verzameling van bepaalde soorten gegevens op elk moment tijdelijk of permanent stop te zetten, tenzij de verwerkingsverantwoordelijke zich op een specifieke rechtsgrond kan beroepen om de verzameling van specifieke gegevens voort te zetten. Bij een overeenkomst die een gepersonaliseerd aanbod omvat op basis van het rijgedrag, is het mogelijk dat de gebruiker als gevolg van de stopzetting weer wordt onderworpen aan de standaardvoorwaarden van de overeenkomst. Deze functies moeten in het voertuig worden vervuld, hoewel ze ook via aanvullende middelen (zoals een specifieke toepassing) aan de betrokkenen kunnen worden verleend. De EDPB beveelt fabrikanten bovendien aan te voorzien in een eenvoudige methode (zoals een verwijderknop) om betrokkenen in staat te stellen snel en gemakkelijk persoonsgegevens te verwijderen die op het dashboard van de auto kunnen worden opgeslagen (bijvoorbeeld de GPS-navigatiegeschiedenis, internethistoriek enz.).

92. Bij de verkoop van een verbonden voertuig en de bijkomende verandering van eigenaar moeten persoonsgegevens die niet langer nodig zijn voor de eerder gespecificeerde doeleinden, worden gewist, en moet de betrokkene zijn of haar recht op overdraagbaarheid kunnen uitoefenen.

2.7 Beveiliging

93. Fabrikanten van voertuigen en van apparatuur, dienstverleners en andere verwerkingsverantwoordelijken moeten maatregelen treffen die de veiligheid en vertrouwelijkheid van de verwerkte gegevens waarborgen en alle zinvolle voorzorgsmaatregelen nemen om te voorkomen dat onbevoegden controle kunnen uitoefenen. De deelnemers uit de sector moeten met name overwegen de volgende maatregelen te nemen:

- Z versleuteling van de communicatiekanalen door middel van een geavanceerd algoritme;
- Z invoering van een systeem voor het beheer van encryptiesleutels dat uniek is voor elk voertuig en niet voor elk model;
- Z versleuteling van op afstand opgeslagen gegevens met behulp van de modernste algoritmen;
- Z regelmatige vernieuwing van encryptiesleutels;
- Z bescherming van encryptiesleutels tegen elke openbaarmaking;
- Z authenticatie van apparatuur waarop gegevens worden ontvangen;
- Z waarborgen van de gegevensintegriteit (bijvoorbeeld door middel van hashing);
- Z de toegang tot persoonsgegevens afhankelijk maken van betrouwbare technieken voor de gebruikerauthenticatie (wachtwoord, elektronisch certificaat enz.).

94. De EDPB beveelt voertuigfabrikanten in het bijzonder aan de volgende beveiligingsmaatregelen uit te voeren:

- Z scheiding van de vitale functies van het voertuig van de functies die altijd afhankelijk zijn van telecommunicatiecapaciteiten (bijvoorbeeld “infotainment”);
- Z uitvoering van technische maatregelen die voertuigfabrikanten in staat stellen kwetsbaarheden in de beveiliging snel te verhelpen gedurende de gehele levensduur van het voertuig;
- Z wat de vitale functies van het voertuig betreft, zoveel mogelijk voorrang geven aan het gebruik van beveiligde communicatiemiddelen die specifiek voor het vervoer bestemd zijn;
- Z opzetting van een alarmsysteem dat waarschuwt bij aanvallen op de systemen van het voertuig, met de mogelijkheid om naar een beperkte bedrijfsmodus over te schakelen⁴⁷;
- Z bijhouden van een logboek waarin elke toegang tot het voertuiginformatiesysteem wordt geregistreerd, dat bijvoorbeeld maximaal zes maanden teruggaat, zodat de oorsprong van elke potentiële aanval kan worden achterhaald en de geregistreeerde informatie periodiek kan worden gecontroleerd om mogelijke onregelmatigheden op te sporen.

95. Deze algemene aanbevelingen moeten worden aangevuld met specifieke voorschriften, rekening houdend met de kenmerken en het doeleinde van elke gegevensverwerking.

⁴⁷ Een beperkte bedrijfsmodus is een modus van het voertuig waarbij de functies die essentieel zijn voor de veilige werking van het voertuig (d.w.z. de minimale veiligheidsvereisten) gewaarborgd blijven, terwijl andere, minder belangrijke functies worden uitgeschakeld (zo kan de werking van het geleidingssysteem als niet-essentieel worden beschouwd, in tegenstelling tot de werking van het remsysteem).

2.8 Doorzending van persoonsgegevens aan derden

96. In principe hebben alleen de verwerkingsverantwoordelijke en de betrokkene toegang tot de gegevens die door een verbonden voertuig worden gegenereerd. De verwerkingsverantwoordelijke kan evenwel persoonsgegevens doorzenden naar een commerciële partner (ontvanger), voor zover die doorzending rechtmatig berust op een van de in artikel 6 AVG genoemde rechtsgronden.
97. Gezien de mogelijke gevoeligheid van de voertuiggebruiksgegevens (bijvoorbeeld afgelegde ritten, rijstijl) beveelt de EDPB aan systematisch de toestemming van de betrokkene te vragen alvorens zijn/haar gegevens door te zenden naar een commerciële partner die optreedt als verwerkingsverantwoordelijke (bijvoorbeeld door een vakje aan te vinken dat niet vooraf is aangevinkt, of, indien technisch mogelijk, door gebruik te maken van een fysieke of logische voorziening waartoe de betrokkene vanuit het voertuig toegang heeft). De commerciële partner wordt op zijn/haar beurt verantwoordelijk voor de gegevens die hij/zij ontvangt en is onderworpen aan alle bepalingen van de AVG.
98. De voertuigfabrikant, dienstverlener of andere verwerkingsverantwoordelijke kan persoonsgegevens doorzenden naar een gegevensverwerker die is geselecteerd om een rol te spelen in de dienstverlening aan de betrokkene, mits de gegevensverwerker die gegevens niet voor eigen doeleinden gebruikt. De verwerkingsverantwoordelijken en de verwerkers stellen een overeenkomst of een ander juridisch document op waarin de verplichtingen van elke partij worden gespecificeerd en waarin de bepalingen van artikel 28 AVG worden uiteengezet.

2.9 Doorgifte van persoonsgegevens buiten de EU/EER

99. Wanneer persoonsgegevens aan een partij buiten de Europese Economische Ruimte worden doorgegeven, gelden er speciale waarborgen om ervoor te zorgen dat de bescherming met de gegevens meereist.
100. Bijgevolg mag de verwerkingsverantwoordelijke persoonsgegevens alleen aan een ontvanger doorgeven voor zover die doorgifte in overeenstemming is met de voorschriften van hoofdstuk V van de AVG.

2.10 Gebruik van wifitechnologieën aan boord van voertuigen

101. Dankzij de vooruitgang in de cellulaire technologie is het makkelijk geworden om onderweg van internet gebruik te maken. Hoewel het mogelijk is een wifiverbinding in een voertuig tot stand te brengen met behulp van een smartphone-hotspot of een speciaal apparaat (OBD-II-dongle, draadloze modem of router enz.), bieden de meeste fabrikanten tegenwoordig modellen aan met een ingebouwde cellulaire gegevensverbinding die ook wifinetwerken kunnen creëren. Afhankelijk van het geval moeten verschillende aspecten in overweging worden genomen:

ZDe wifiverbinding wordt als dienst aangeboden door een beroepsbeoefenaar op de weg, zoals een taxichauffeur voor zijn/haar klanten. In dit geval kan de beroepsbeoefenaar of zijn/haar bedrijf worden beschouwd als een internetaanbieder die zodoende onderworpen is aan specifieke verplichtingen en beperkingen met betrekking tot de verwerking van de persoonsgegevens van zijn/haar klanten.

ZDe wifiverbinding is uitsluitend bedoeld voor gebruik door de bestuurder (uitsluitend voor de bestuurder en zijn/haar passagiers). In dit geval wordt de verwerking van persoonsgegevens beschouwd als een zuiver persoonlijke of huishoudelijke activiteit in de zin van artikel 2, lid 2, punt c), en overweging 18 van de AVG.

102. In het algemeen houdt de grootschalige verspreiding van interfaces voor wifi-internetverbindingen grotere risico's in voor de persoonlijke levenssfeer van personen. Door hun voertuigen worden gebruikers immers continue zenders, en kunnen zij dus worden

geïdentificeerd en getraceerd. Om tracing te voorkomen, moeten de fabrikanten van voertuigen en van apparatuur daarom gebruiksvriendelijke opt-out-opties bieden die ervoor zorgen dat de service set identifier (SSID) van het wifinetwerk aan boord niet wordt verzameld.

3 CASESTUDY'S

103. In dit deel worden vijf specifieke voorbeelden van verwerking in het kader van verbonden voertuigen behandeld, die overeenstemmen met scenario's waarmee belanghebbenden in de sector vaak te maken krijgen. De voorbeelden betreffen gegevensverwerking waarvoor rekenkracht nodig is die niet lokaal in het voertuig kan worden ingezet en/of waarbij persoonsgegevens worden doorgestuurd naar een derde partij om verdere analyses te verrichten of om verdere functionaliteit op afstand te bieden. Voor elk type verwerking worden in dit document de beoogde doeleinden, de categorieën van verzamelde gegevens, de bewaartermijn van die gegevens, de rechten van de betrokkenen, de te nemen beveiligingsmaatregelen en de ontvangers van de informatie gespecificeerd. Indien sommige van deze aspecten hieronder niet aan bod komen, gelden de in het vorige deel beschreven algemene aanbevelingen.
104. De gekozen voorbeelden zijn niet uitputtend en zijn bedoeld om te illustreren welke verscheidenheid aan soorten verwerking, rechtsgronden, actoren enz. in het kader van verbonden voertuigen kan voorkomen.

3.1 Verlening van een dienst door een derde

105. Betrokkenen kunnen bij een dienstverlener diensten afnemen die een meerwaarde bieden met betrekking tot hun voertuig. Zo kan de betrokkene een op het gebruik gebaseerde verzekeringsovereenkomst sluiten die voorziet in lagere verzekeringspremies wanneer hij/zij minder rijdt ("Pay As You Drive") of goed rijgedrag vertoont ("Pay How You Drive") en waarvoor het rijgedrag moet worden gemonitord door de verzekeringsmaatschappij. De betrokkene kan ook een overeenkomst sluiten met een bedrijf dat pechhulp aanbiedt, waarbij de locatie van het voertuig wordt doorgegeven aan het bedrijf of aan een dienstverlener om berichten of waarschuwingen over de werking van het voertuig te ontvangen (zoals een waarschuwing over de slijtage van de remmen, of een herinnering aan de datum van de technische keuring).

3.1.1 Verzekering op basis van gebruik

106. "Pay as you drive" is een vorm van verzekering op basis van verbruik waarbij het aantal afgelegde kilometers en/of de rijgewoonten van de bestuurder worden bijgehouden om "veilige" bestuurders te onderscheiden en te belonen met een lagere premie. De verzekeraar eist dat de bestuurder een ingebouwde telematicadienst of een mobiele applicatie installeert of een ingebouwde module van de fabrikant activeert die het aantal afgelegde kilometers en/of het rijgedrag (rempatroon, optreksnelheid enz.) van de verzekeringnemer bijhoudt. Aan de hand van de door het telematicasysteem verzamelde informatie worden aan de bestuurder scores toegekend om te analyseren welke risico's hij/zij voor de verzekeringsmaatschappij kan vormen.
107. Aangezien voor een verzekering op basis van gebruik toestemming is vereist uit hoofde van artikel 5, lid 3, van de e-privacyrichtlijn, wijst de EDPB erop dat de verzekeringnemer de keuze moet hebben om een niet op het gebruik gebaseerde verzekering af te sluiten. Anders kan de toestemming niet worden beschouwd als vrijelijk gegeven, aangezien de uitvoering van de overeenkomst afhankelijk zou zijn van de toestemming. Voorts bepaalt artikel 7, lid 3, AVG, dat een betrokkene het recht heeft zijn/haar toestemming in te trekken.

3.1.1.1 Rechtsgrond

108. Wanneer de gegevens worden verzameld via een openbaar beschikbare elektronische-communicatiedienst (bijvoorbeeld via de simkaart in het telematicasysteem), is toestemming nodig om toegang te krijgen tot informatie die reeds in het voertuig is opgeslagen, zoals bepaald in artikel 5, lid 3, van de e-privacyrichtlijn. In deze context kan derhalve geen van de bij deze bepalingen verleende vrijstellingen worden toegepast: de verwerking heeft niet uitsluitend ten doel een communicatie te verzenden over een elektronisch communicatienetwerk en houdt geen verband met een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij. De toestemming kan worden verkregen op het moment waarop de overeenkomst wordt gesloten.
109. Wat betreft de verwerking van persoonsgegevens na de opslag van of de toegang tot de eindapparatuur van de eindgebruiker, kan de verzekeringsmaatschappij zich in deze specifieke context beroepen op artikel 6, lid 1, punt b), van de AVG, mits zij kan aantonen dat de verwerking plaatsvindt in het kader van een geldige overeenkomst met de betrokkene en dat de verwerking noodzakelijk is om de specifieke overeenkomst met de betrokkene te kunnen uitvoeren. Voor zover de verwerking objectief noodzakelijk is voor de uitvoering van de overeenkomst met de betrokkene, is de EDPB van oordeel dat een beroep op artikel 6, lid 1, punt b), van de AVG niet tot gevolg zou hebben dat de aanvullende bescherming van artikel 5, lid 3, van de e-privacyrichtlijn wordt verminderd. Deze rechtsgrond wordt verwezenlijkt doordat de betrokkene een overeenkomst ondertekent met de verzekeringsmaatschappij.

3.1.1.2 Verzamelde gegevens

110. Er moeten twee soorten persoonsgegevens in aanmerking worden genomen:

- Z **commerciële en transactionele gegevens:** identificatiegegevens van de betrokkene, gegevens betreffende transacties, gegevens betreffende betaalmiddelen enz.;
- Z **gebruiksgegevens:** persoonsgegevens die door het voertuig worden gegenereerd, rijgewoonten, locatie enz.

111. Aangezien het risico bestaat dat de via de telematicabox verzamelde gegevens worden misbruikt om een nauwkeurig profiel van de bewegingen van de bestuurder op te stellen, beveelt de EDPB aan om de ruwe gegevens betreffende het rijgedrag voor zover mogelijk te verwerken:

- Z in het voertuig in telematicaboxen of in de smartphone van de gebruiker, zodat de verzekeraar alleen toegang heeft tot de resultaatgegevens (bijvoorbeeld een score met betrekking tot het rijgedrag), en niet tot gedetailleerde ruwe gegevens (zie punt 2.1);
- Z of door een telematicadienstverlener namens de verwerkingsverantwoordelijke (de verzekeringsmaatschappij) om numerieke scores te genereren die op een welbepaalde manier aan de verzekeringsmaatschappij worden doorgegeven. In dit geval moeten ruwe gegevens en gegevens die rechtstreeks verband houden met de identiteit van de bestuurder van elkaar worden gescheiden. Dit betekent dat de telematicadienstverlener de gegevens in realtime ontvangt, maar niet de namen, kentekens enz. van de polishouders kent. Anderzijds kent de verzekeraar de namen van de polishouders, maar ontvangt hij alleen de scores en het totale aantal kilometers en niet de ruwe gegevens die worden gebruikt om deze scores op te stellen.

112. Er mogen overigens geen locatiegegevens worden verzameld indien alleen het aantal kilometers noodzakelijk is voor de uitvoering van de overeenkomst.

3.1.1.3 Bewaringstermijn

113. In het kader van gegevensverwerking die plaatsvindt om een overeenkomst uit te voeren (d.w.z. verlening van een dienst), is het van belang onderscheid te maken tussen twee soorten gegevens alvorens hun respectieve bewaringstermijnen vast te stellen:

- Z **Commerciële en transactionele gegevens:** die gegevens kunnen in een actieve gegevensbank worden bewaard voor de volledige duur van de overeenkomst. Aan het einde van de overeenkomst kunnen zij fysiek worden gearchiveerd (op een afzonderlijke drager zoals een dvd) of logisch worden gearchiveerd (door autorisatiebeheer) in geval van eventuele geschillen. Vervolgens worden de gegevens aan het einde van de wettelijke verjaringstermijnen gewist of geanonimiseerd.
- Z **Gebruiksgegevens:** gebruiksgegevens kunnen worden ingedeeld in ruwe gegevens en geaggregeerde gegevens. Zoals hierboven vermeld, mogen de verwerkingsverantwoordelijken of de verwerkers, indien mogelijk, geen ruwe gegevens verwerken. Indien dat toch noodzakelijk is, mogen onbewerkte gegevens slechts zo lang worden bewaard als nodig is om de geaggregeerde gegevens op te stellen en de geldigheid van dat aggregatieproces te controleren. Geaggregeerde gegevens mogen zo lang worden bewaard als nodig is voor het verlenen van de dienst of anderszins door het Unierecht of het recht van de lidstaten wordt verlangd.

3.1.1.4 *Informatieverstrekking aan en rechten van betrokkenen*

114. Voordat persoonsgegevens worden verwerkt, wordt de betrokkene overeenkomstig artikel 13 van de AVG op transparante en begrijpelijke wijze geïnformeerd. Hij of zij moet met name worden geïnformeerd over de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn. In dit laatste geval beveelt de EDPB aan een pedagogische aanpak te volgen om het verschil te benadrukken tussen ruwe gegevens en de score die op basis daarvan wordt geproduceerd, en daarbij te benadrukken dat de verzekeraar in voorkomend geval alleen het resultaat van de score zal verzamelen.
115. Wanneer de gegevens niet in het voertuig worden verwerkt, maar door een telematicadienstverlener namens de verwerkingsverantwoordelijke (de verzekeringsmaatschappij), kan het nuttig zijn in de informatie te vermelden dat de dienstverlener in dit geval geen toegang heeft tot gegevens die rechtstreeks verband houden met de identiteit van de bestuurder (zoals namen, nummerplaten enz.). Gelet op het belang om betrokkenen te informeren over de gevolgen van de verwerking van hun persoonsgegevens en op het feit dat betrokkenen niet mogen worden verrast door de verwerking van hun persoonsgegevens, beveelt de EDPB ook aan om betrokkenen te informeren over het bestaan van profilering en de gevolgen daarvan, zelfs als daarbij geen geautomatiseerde besluitvorming plaatsvindt als bedoeld in artikel 22 AVG.
116. Betrokkenen moeten, gelet op hun rechten, specifiek worden geïnformeerd over de beschikbare middelen om hun recht van inzage, rectificatie, beperking en wissing uit te oefenen. Aangezien de in dit verband verzamelde gegevens door de betrokkene zelf worden verstrekt (via specifieke formulieren of via zijn/haar activiteiten) en worden verwerkt op basis van artikel 6, lid 1, punt b), AVG (uitvoering van een overeenkomst), is de betrokkene gerechtigd zijn of haar recht op gegevensoverdraagbaarheid uit te oefenen. Zoals in de richtsnoeren betreffende het recht op gegevensoverdraagbaarheid wordt benadrukt, beveelt de EDPB ten stelligste aan dat de verwerkingsverantwoordelijken duidelijk het verschil uitleggen tussen de soorten gegevens die een betrokkene kan ontvangen op grond van het recht van toegang tot zijn gegevens en het recht van gegevensoverdraagbaarheid⁴⁸.
117. De informatie kan worden verstrekt bij de ondertekening van de overeenkomst.

⁴⁸ Groep gegevensbescherming artikel 29, Richtlijnen inzake het recht op gegevensoverdraagbaarheid, WP242 rev.01, bekrachtigd door de EDPB, blz. 13.

3.1.1.5 *Ontvanger:*

118. De EDPB beveelt aan de gebruiksgegevens van het voertuig zoveel mogelijk rechtstreeks in telematicaboxen te verwerken, zodat de verzekeraar alleen toegang heeft tot de resultaatgegevens (bijvoorbeeld een score) en niet tot gedetailleerde ruwe gegevens.
119. Indien een telematicadienstverlener de gegevens namens de verwerkingsverantwoordelijke (de verzekeringsmaatschappij) verzamelt om numerieke scores te genereren, hoeft hij/zij de identiteit van de bestuurder (zoals namen, kentekens enz.) van de polishouders niet te kennen.

3.1.1.6 *Veiligheid:*

120. Hier gelden de algemene aanbevelingen. Zie punt 2.7.

3.1.2 Een parkeerplaats huren en reserveren

121. De eigenaar van een parkeerplaats wil die wellicht verhuren. Hij meldt een parkeerplaats aan en stelt een tarief vast op een onlinetoepassing. Zodra de parkeerplaats is aangemeld, stelt de toepassing de eigenaar in kennis wanneer een bestuurder de parkeerplaats wil reserveren. De bestuurder kan een bestemming selecteren en op basis van meerdere criteria controleren of er een parkeerplaats beschikbaar is. Na de goedkeuring van de eigenaar wordt de transactie bevestigd en handelt de dienstverlener de betalingstransactie af, waarna de bestuurder met behulp van het navigatiesysteem naar de locatie rijdt.

3.1.2.1 *Rechtsgrond*

122. Wanneer de gegevens worden verzameld via een openbare elektronische-communicatiedienst, is artikel 5, lid 3, van de e-privacyrichtlijn van toepassing.
123. Aangezien het een dienst van de informatiemaatschappij betreft, is op grond van artikel 5, lid 3, van de e-privacyrichtlijn geen toestemming vereist om toegang te krijgen tot informatie die reeds in het voertuig is opgeslagen, wanneer de abonnee uitdrukkelijk om een dergelijke dienst verzoekt.
124. Voor de verwerking van persoonsgegevens en alleen voor gegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst waarbij de betrokkene partij is, is artikel 6, lid 1, punt b), AVG de rechtsgrond.

3.1.2.2 *Verzamelde gegevens*

125. De verwerkte gegevens omvatten de contactgegevens van de bestuurder (naam, e-mail, telefoonnummer, voertuigtype [bijvoorbeeld auto, vrachtwagen, motorfiets], kenteken, parkeerperiode, betalingsgegevens [zoals kredietkaartgegevens]), alsook navigatiegegevens.

3.1.2.3 *Bewaringstermijn*

126. De gegevens mogen slechts zo lang worden bewaard als nodig is om de parkeerovereenkomst uit te voeren of anderszins door het recht van de Unie of de lidstaten wordt voorgeschreven. Daarna worden de gegevens ofwel geanonimiseerd ofwel gewist.

3.1.2.4 *Informatieverstrekking aan en rechten van betrokkenen*

127. Voordat persoonsgegevens worden verwerkt, wordt de betrokkene overeenkomstig artikel 13 van de AVG op transparante en begrijpelijke wijze geïnformeerd.
128. De betrokkene moet specifiek worden geïnformeerd over de beschikbare middelen om zijn/haar recht van inzage, rectificatie, beperking en wissing uit te oefenen. Aangezien de in dit verband verzamelde gegevens voorts door de betrokkene zelf worden verstrekt (via specifieke formulieren of via zijn/haar activiteiten) en worden verwerkt op basis van artikel 6, lid 1, punt b), AVG (uitvoering van een overeenkomst), is de betrokkene gerechtigd zijn of haar recht op gegevensoverdraagbaarheid uit te oefenen. Zoals in de richtsnoeren betreffende het recht op gegevensoverdraagbaarheid wordt benadrukt, beveelt de EDPB

ten stelligste aan dat de verwerkingsverantwoordelijken duidelijk het verschil uitleggen tussen de soorten gegevens die een betrokkene kan ontvangen op grond van het recht van toegang tot zijn gegevens en het recht van gegevensoverdraagbaarheid.

3.1.2.5 Ontvanger:

129. In principe hebben alleen de verwerkingsverantwoordelijke en de verwerker toegang tot de gegevens.

3.1.2.6 Veiligheid:

130. Hier gelden de algemene aanbevelingen. Zie punt 2.7.

3.2 eCall

131. Bij een ernstig ongeval in de Europese Unie activeert het voertuig automatisch een eCall naar 112, het EU-brede noodnummer (zie punt 1.1 voor meer details), zodat snel een ambulance naar de plaats van het ongeval kan worden gestuurd overeenkomstig Verordening (EU) 2015/758 van het Europees Parlement en de Raad van 29 april 2015 inzake typegoedkeuringseisen voor de uitrol van het op de 112-dienst gebaseerde eCall-boordsysteem en houdende wijziging van Richtlijn 2007/46/EG (hierna: "Verordening (EU) 2015/758").
132. De in het voertuig geïnstalleerde eCall-generator, die toezending van gegevens via een openbaar mobiel draadloos communicatienetwerk mogelijk maakt, initieert een noodoproep, die automatisch door voertuigsensoren of handmatig door de inzittenden in werking wordt gesteld wanneer sprake is van een ongeval. Naast de activering van het audiokanaal wordt bij een ongeval automatisch een minimumreeks van gegevens (Minimum Set of Data — MSD) gegenereerd en naar de alarmcentrale verzonden.

3.2.1 Rechtsgrond

133. Wat de toepassing van de e-privacyrichtlijn betreft, moeten twee bepalingen in aanmerking worden genomen:
 - Z artikel 9 betreffende andere locatiegegevens dan verkeersgegevens, dat alleen van toepassing is op elektronische-communicatiediensten;
 - Z artikel 5, lid 3, voor het verkrijgen van toegang tot informatie die is opgeslagen in de generator die in het voertuig is geïnstalleerd.
134. Hoewel deze bepalingen in beginsel de toestemming van de betrokkene vereisen, brengt Verordening (EU) 2015/758 voor de verwerkingsverantwoordelijke een wettelijke verplichting met zich mee (de betrokkene heeft geen echte of vrije keuze en kan de verwerking van zijn/haar gegevens niet weigeren). Verordening (EU) 2015/758 heeft dus voorrang op de noodzaak van toestemming van de bestuurder voor de verwerking van locatiegegevens en de minimumreeks van gegevens⁴⁹.
135. De naleving van een wettelijke verplichting vormt de rechtsgrond voor de verwerking van die gegevens, zoals bepaald in artikel 6, lid 1, punt c), AVG (d.w.z. Verordening (EU) 2015/758).

⁴⁹ Artikel 8, lid 1, punt f), van het onderhandelingsmandaat van de Raad voor het voorstel voor een e-privacyverordening voorziet overigens in een specifieke vrijstelling voor eCall, aangezien toestemming niet nodig is wanneer "de bedoelde handelingen overeenkomstig artikel 13, lid 3, nodig zijn om de eindapparatuur te lokaliseren wanneer een eindgebruiker een noodcommunicatie verricht naar het uniform Europees alarmnummer "112" of een nationaal noodnummer.

3.2.2 Verzamelde gegevens

136. In Verordening (EU) 2015/758 is bepaald dat de gegevens die door het op 112 gebaseerde eCall-boordsysteem worden doorgezonden, slechts de minimuminformatie bevatten als bedoeld in de norm EN 15722:2011 "Intelligent transport systems — eSafety — eCall minimum set of data (MSD)", met inbegrip van:

- Z de aanduiding of eCall handmatig of automatisch in werking is gesteld;
- Z het voertuigtype;
- Z het identificatienummer van het voertuig (VIN);
- Z het type aandrijving van het voertuig;
- Z het tijdstip waarop het initiële gegevensbericht in het kader van de huidige eCall-oproep is gegenereerd;
- Z de laatst bekende positie in lengte- en breedtegraad van het voertuig, bepaald op het laatst mogelijke moment voor het genereren van het bericht;
- Z de laatst bekende werkelijke rijrichting van het voertuig, bepaald op het laatst mogelijke moment voor het genereren van het bericht (alleen de laatste drie locaties van het voertuig).

3.2.3 Bewaringstermijn

137. In Verordening (EU) 2015/758 is bepaald dat gegevens niet langer mogen worden bewaard dan nodig is voor de afhandeling van noodsituaties. Die gegevens worden volledig gewist zodra zij voor die afhandeling niet langer nodig zijn. Bovendien worden de gegevens in het interne geheugen van het eCall-boordsysteem automatisch en voortdurend verwijderd. Alleen de laatste drie locaties van het voertuig mogen worden bijgehouden voor zover dat strikt noodzakelijk is voor het bepalen van de huidige locatie en de rijrichting op het ogenblik van de noodsituatie.

3.2.4 Informatieverstrekking aan en rechten van betrokkenen

138. In artikel 6 van Verordening (EU) 2015/758 is bepaald dat de fabrikanten duidelijke en uitgebreide informatie verstrekken over de verwerking van de gegevens die via het eCall-systeem zijn verstuurd. Deze informatie wordt in de gebruikershandleiding afzonderlijk verstrekt voor het op 112 gebaseerde eCall-boordsysteem en de door diensten van derden ondersteunde eCall-systemen, voordat het systeem in gebruik wordt genomen. De informatie omvat:

- Z de rechtsgrondslag voor de verwerking;
- Z het feit dat standaard het op 112 gebaseerde eCall-boordsysteem wordt geactiveerd;
- Z de voorzieningen van gegevensverwerking door het op 112 gebaseerde eCall-boordsysteem;
- Z het specifieke doel van eCall-verwerking, dat beperkt blijft tot de in de eerste alinea van artikel 5, lid 2, van Verordening (EU) 2015/758 bedoelde noodsituaties;
- Z het type gegevens dat wordt verzameld en verwerkt en de ontvangers van die gegevens;
- Z de termijn voor bewaring van de gegevens in het op 112 gebaseerde eCall-boordsysteem;
- Z het feit dat het voertuig niet permanent wordt gevolgd;
- Z de voorzieningen waaronder degenen op wie de gegevens betrekking hebben hun rechten kunnen doen gelden, alsmede de verantwoordelijke dienst waarmee contact kan worden opgenomen inzake de behandeling van toegangsverzoeken;

Z eventuele noodzakelijke aanvullende informatie omtrent de traceerbaarheid, het volgen en de verwerking van persoonsgegevens in verband met het verlenen van eCall-diensten van derden (third-party service — TPS) en/of andere diensten met toegevoegde waarde, waarvoor de eigenaar zijn/haar uitdrukkelijke toestemming moet verlenen en die in overeenstemming moet zijn met de AVG. In het bijzonder wordt er rekening mee gehouden dat er verschillen kunnen bestaan tussen de gegevensverwerking door het op 112 gebaseerde eCall-boordsysteem en de gegevensverwerking door TPS eCall-boordsystemen of andere diensten met toegevoegde waarde.

139. Voorts verstrekt de dienstverlener de betrokkenen ook transparante en begrijpelijke informatie overeenkomstig artikel 13 AVG. In het bijzonder moet hij of zij worden geïnformeerd over de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook over het feit dat de verwerking van persoonsgegevens is gebaseerd op een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
140. Verder moet, rekening houdend met de aard van de verwerking, de informatie over de ontvangers of categorieën van ontvangers van de persoonsgegevens duidelijk zijn en moeten de betrokkenen ervan in kennis worden gesteld dat de gegevens vóór activering van de eCall niet buiten het op 112 gebaseerde eCall-boordsysteem beschikbaar zijn voor entiteiten.
141. Wat de rechten van de betrokkenen betreft, moet worden opgemerkt dat, aangezien de verwerking op een wettelijke verplichting berust, het recht van bezwaar en het recht op overdraagbaarheid niet van toepassing zijn.

3.2.5 Ontvanger:

142. De gegevens zijn vóór activering van de eCall niet buiten het op 112 gebaseerde eCall-boordsysteem beschikbaar voor entiteiten.
143. Bij activering (hetzij handmatig door de inzittenden van het voertuig, hetzij automatisch zodra een sensor in het voertuig een ernstige botsing detecteert) brengt het eCall-systeem een spraakverbinding tot stand met de desbetreffende alarmcentrale en wordt de minimumreeks van gegevens naar de beheerder van de alarmcentrale gestuurd.
144. Bovendien kunnen gegevens die via het op 112 gebaseerde eCall-boordsysteem worden verstuurd en door de alarmcentrales worden verwerkt, alleen aan de in Besluit nr. 585/2014/EU genoemde noodhulpdiensten en dienstverleningspartners worden overgedragen in geval van incidenten met betrekking tot eCalls en onder de in dat besluit genoemde voorwaarden en zijn zij uitsluitend bedoeld voor het verwezenlijken van de doelstellingen van dat besluit. De door de alarmcentrales via het op 112 gebaseerde eCall-boordsysteem verwerkte gegevens worden niet aan derden overgedragen zonder voorafgaande uitdrukkelijke instemming van de betrokkene.

3.2.6 Beveiliging

145. Bij Verordening (EU) 2015/758 zijn de vereisten vastgesteld om privacybevorderende technologieën te integreren in het eCall-systeem, om de gebruikers van eCall het passende niveau van bescherming van hun privacy te bieden en de nodige garanties te verschaffen ter voorkoming van surveillance en misbruik. Bovendien moeten de fabrikanten ervoor zorgen dat het op 112 gebaseerde eCall-systeem en eventuele andere systemen die een door derden afgehandelde eCall of een dienst met toegevoegde waarde verlenen, zodanig zijn ontworpen dat er tussen die systemen geen uitwisseling van persoonsgegevens mogelijk is.
146. De lidstaten moeten er wat de alarmcentrales betreft met name op toezien dat persoonsgegevens worden beschermd tegen misbruik, met inbegrip van onrechtmatige toegang, wijziging of verlies, en dat protocollen betreffende opslag, bewaringstermijn,

verwerking en bescherming van persoonsgegevens op het juiste niveau worden opgesteld en naar behoren in acht worden genomen.

3.3 Bestudering van oorzaken en gevolgen van ongevallen

147. Betrokkenen kunnen vrijwillig deelnemen aan een onderzoek waarbij de oorzaken en gevolgen van ongevallen worden bestudeerd, waarmee een beter begrip van de oorzaken van verkeersongevallen en algemenere wetenschappelijke doeleinden worden nagestreefd.

3.3.1 Rechtsgrond

148. Wanneer de gegevens worden verzameld via een openbare elektronische-communicatiedienst, heeft de verwerkingsverantwoordelijke toestemming van de betrokkene nodig om toegang te verkrijgen tot informatie die reeds is opgeslagen in het voertuig, zoals bepaald in artikel 5, lid 3, van de e-privacyrichtlijn. In deze context kan derhalve geen van de bij deze bepalingen verleende vrijstellingen worden toegepast: de verwerking heeft niet uitsluitend ten doel een communicatie te verzenden over een elektronisch communicatienetwerk en houdt geen verband met een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij.
149. Rekening houdend met de grote hoeveelheid aan uiteenlopende persoonsgegevens die nodig zijn om de oorzaken en gevolgen van ongevallen te bestuderen, beveelt de EDPB aan de verwerking van persoonsgegevens te koppelen aan de voorafgaande toestemming van de betrokkene overeenkomstig artikel 6 AVG. Die voorafgaande toestemming moet worden gegeven op een specifiek formulier, waarmee de betrokkene zich vrijwillig opgeeft om aan de studie deel te nemen en zijn of haar persoonsgegevens voor dat doel te laten verwerken. Toestemming is een vrije, specifieke en geïnformeerde wilsuiting van de persoon wiens gegevens worden verwerkt (bijvoorbeeld door een vakje aan te vinken dat niet vooraf is aangevinkt, of de boordcomputer te configureren om een functie in het voertuig te activeren). Deze toestemming moet afzonderlijk en voor specifieke doeleinden worden gegeven, mag niet worden gebundeld met de koop- of leasingovereenkomst voor een nieuwe auto en moet even gemakkelijk kunnen worden ingetrokken als zij is gegeven. Wanneer de toestemming wordt ingetrokken, wordt de verwerking stopgezet. De gegevens worden dan uit de actieve gegevensbank verwijderd of geanonimiseerd.
150. De toestemming die nodig is uit hoofde van artikel 5, lid 3, van de e-privacyrichtlijn en de toestemming die nodig is als rechtsgrond voor de verwerking van gegevens kunnen tegelijkertijd worden verkregen (bijvoorbeeld door een vakje aan te vinken waarin duidelijk wordt aangegeven waarmee de betrokkene instemt).
151. Er zij op gewezen dat, afhankelijk van de verwerkingsvoorwaarden (de aard van de verwerkingsverantwoordelijke enz.), rechtmatig een andere rechtsgrond mag worden gekozen, zolang die de aanvullende bescherming van artikel 5, lid 3, van de e-privacyrichtlijn niet vermindert (zie punt 15). Indien de verwerking op een andere rechtsgrond berust, zoals de vervulling van een taak van algemeen belang (artikel 6, lid 1, punt e), AVG), beveelt de EDPB aan dat de betrokkenen op vrijwillige basis in de studie worden opgenomen.

3.3.2 Verzamelde gegevens

152. De verwerkingsverantwoordelijke verzamelt uitsluitend persoonsgegevens die strikt noodzakelijk zijn voor de verwerking.
153. Er moeten twee soorten gegevens in aanmerking worden genomen:
 - Z gegevens met betrekking tot deelnemers en voertuigen;**
 - Z technische voertuiggegevens** (momentane snelheid enz.).
154. Wetenschappelijk onderzoek waarbij de oorzaken en gevolgen van ongevallen worden onderzocht, vormt een rechtvaardiging voor het verzamelen van de momentane snelheid, ook door rechtspersonen die geen openbare dienst in strikte zin beheren.
155. Zoals hierboven is opgemerkt, is de EDPB van mening dat de gegevens over de momentane snelheid die in het kader van een studie naar de oorzaken en gevolgen van ongevallen worden verzameld, geen gegevens zijn met het oog op strafvervolging (d.w.z. dat zij niet worden verzameld om een strafbaar feit te onderzoeken of tot vervolging over te gaan), waardoor de verzameling ervan door rechtspersonen die geen openbare dienst in strikte zin beheren, gerechtvaardigd is.

3.3.3 Bewaringstermijn

156. Het is van belang een onderscheid te maken tussen twee soorten gegevens. Ten eerste kunnen de gegevens met betrekking tot de deelnemers en de voertuigen voor de duur van de studie worden bewaard. Ten tweede moeten de technische voertuiggegevens zo kort mogelijk worden bewaard als nodig is voor het doeleinde. In dit verband lijkt vijf jaar vanaf de einddatum van de studie een redelijke termijn. Aan het eind van die periode moeten de gegevens worden gewist of geanonimiseerd.

3.3.4 Informatieverstrekking aan en rechten van betrokkenen

157. Voordat persoonsgegevens worden verwerkt, wordt de betrokkene overeenkomstig artikel 13 van de AVG op transparante en begrijpelijke wijze geïnformeerd. Met name in het geval van het verzamelen van momentane snelheden moeten de betrokkenen specifiek worden geïnformeerd over het verzamelen van gegevens. Aangezien de gegevensverwerking op toestemming berust, moet de betrokkene specifiek worden geïnformeerd over het bestaan van het recht om zijn/haar toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan. Aangezien de in dit verband verzamelde gegevens voorts door de betrokkene zelf worden verstrekt (via specifieke formulieren of via zijn/haar activiteiten) en worden verwerkt op basis van artikel 6, lid 1, punt a), AVG (toestemming), is de betrokkene gerechtigd zijn of haar recht op gegevensoverdraagbaarheid uit te oefenen. Zoals in de richtsnoeren betreffende het recht op gegevensoverdraagbaarheid wordt benadrukt, beveelt de EDPB ten stelligste aan dat de verwerkingsverantwoordelijken duidelijk het verschil uitleggen tussen de soorten gegevens die een betrokkene kan ontvangen op grond van het recht van toegang tot zijn gegevens en het recht van gegevensoverdraagbaarheid. Bijgevolg moet de verwerkingsverantwoordelijke de betrokkene een gemakkelijke manier bieden om zijn of haar toestemming, vrijelijk en te allen tijde, in te trekken, en instrumenten ontwikkelen om te kunnen ingaan op verzoeken om gegevensoverdraagbaarheid.
158. Die informatie kan worden verstrekt na ondertekening van het formulier waarmee men instemt met deelname aan de studie naar de oorzaken en gevolgen van het ongeval.

3.3.5 Ontvanger

159. In principe hebben alleen de verwerkingsverantwoordelijke en de verwerker toegang tot de gegevens.

3.3.6 Beveiliging

160. Zoals hierboven opgemerkt, moeten de getroffen beveiligingsmaatregelen worden afgestemd op de mate van gevoeligheid van de gegevens. Indien bijvoorbeeld gegevens over de momentane snelheid (of andere gegevens in verband met strafrechtelijke veroordelingen en strafbare feiten) worden verzameld in het kader van de studie naar de oorzaken en gevolgen van het ongeval, beveelt de EDPB ten zeerste aan krachtige beveiligingsmaatregelen te treffen, zoals:

- Z pseudonimisering (bijvoorbeeld hashing van gegevens met geheime sleutels, zoals de achternaam/voornaam van de betrokkene en het serienummer);
- Z de opslag van gegevens over de momentane snelheid en over de locatie in afzonderlijke gegevensbanken (bijvoorbeeld met behulp van een geavanceerd encryptiemechanisme met verschillende sleutels en goedkeuringsmechanismen);
- Z en/of het wissen van locatiegegevens zodra de betreffende gebeurtenis of sequentie is geclassificeerd (bijvoorbeeld het wegtype, dag/nacht), en de opslag van direct identificeerbare gegevens in een afzonderlijke gegevensbank die slechts door een klein aantal personen kan worden geraadpleegd.

3.4 Bestrijding van autodiefstal

161. Betrokkenen kunnen in geval van diefstal op zoek gaan naar hun voertuig aan de hand van locatiegegevens. Het gebruik van locatiegegevens is beperkt tot wat strikt noodzakelijk is in het kader van het onderzoek en tot de beoordeling van de zaak door de bevoegde rechterlijke instanties.

3.4.1 Rechtsgrond

162. Wanneer de gegevens worden verzameld via een openbare elektronische-communicatiedienst, is artikel 5, lid 3, van de e-privacyrichtlijn van toepassing.
163. Aangezien het een dienst van de informatiemaatschappij betreft, is op grond van artikel 5, lid 3, van de e-privacyrichtlijn geen toestemming vereist om toegang te krijgen tot informatie die reeds in het voertuig is opgeslagen, wanneer de abonnee uitdrukkelijk om een dergelijke dienst verzoekt.
164. Wat de verwerking van persoonsgegevens betreft, vormt de toestemming van de voertuigeigenaar of, in voorkomend geval, de uitvoering van een overeenkomst (alleen voor de gegevens die nodig zijn voor de uitvoering van de overeenkomst waarbij de eigenaar van het voertuig partij is) de rechtsgrond voor de verwerking van locatiegegevens.
165. Toestemming is een vrije, specifieke en geïnformeerde wilsuiting van de persoon wiens gegevens worden verwerkt (bijvoorbeeld het aanvinken van een vakje dat niet vooraf is aangevinkt, of het configureren van de boordcomputer om een functie in het voertuig te activeren). De vrijheid om toestemming te verlenen houdt in dat de betrokkene te allen tijde zijn toestemming kan intrekken; de betrokkene moet hiervan uitdrukkelijk in kennis worden gesteld. Wanneer de toestemming wordt ingetrokken, wordt de verwerking stopgezet. De gegevens moeten dan uit de actieve gegevensbank worden verwijderd, worden geanonimiseerd, of worden gearchiveerd.

3.4.2 Verzamelde gegevens

166. Locatiegegevens mogen alleen worden doorgezonden vanaf de aangifte van diefstal, en mogen de rest van de tijd niet continu worden verzameld.

3.4.3 Bewaringstermijn

167. Locatiegegevens mogen slechts worden bewaard gedurende de periode waarin de zaak door de bevoegde rechterlijke instanties wordt beoordeeld, of tot het einde van een procedure om twijfel weg te nemen die niet eindigt met de bevestiging van de diefstal van het voertuig.

3.4.4 Informatieverstrekking aan betrokkenen

168. Voordat persoonsgegevens worden verwerkt, wordt de betrokkene overeenkomstig artikel 13 van de AVG op transparante en begrijpelijke wijze geïnformeerd. Meer in het bijzonder beveelt de EDPB aan dat de verwerkingsverantwoordelijke benadrukt dat het voertuig niet permanent wordt gevolgd en dat locatiegegevens pas vanaf de aangifte van diefstal kunnen worden verzameld en doorgezonden. Bovendien moet de verwerkingsverantwoordelijke de betrokkene informeren dat alleen erkende functionarissen van het platform voor bewaking op afstand en wettelijk erkende autoriteiten toegang hebben tot de gegevens.
169. Ten aanzien van de rechten van de betrokkenen moet de betrokkene, wanneer de gegevensverwerking op toestemming berust, specifiek worden geïnformeerd over het bestaan van het recht om zijn/haar toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan. Wanneer de in dit verband verzamelde gegevens door de betrokkene zelf worden verstrekt (via specifieke formulieren of via zijn/haar activiteiten) en worden verwerkt op basis van artikel 6, lid 1, punt a) (toestemming) of artikel 6, lid 1, punt b), AVG

(uitvoering van een overeenkomst), is de betrokkene gerechtigd zijn of haar recht op gegevensoverdraagbaarheid uit te oefenen. Zoals in de richtsnoeren betreffende het recht op gegevensoverdraagbaarheid wordt benadrukt, beveelt de EDPB ten stelligste aan dat de verwerkingsverantwoordelijken duidelijk het verschil uitleggen tussen de soorten gegevens die een betrokkene kan ontvangen op grond van het recht van toegang tot zijn gegevens en het recht van gegevensoverdraagbaarheid.

170. Bijgevolg moet de verwerkingsverantwoordelijke de betrokkene een gemakkelijke manier bieden om zijn/haar toestemming (alleen indien toestemming de rechtsgrond vormt), vrijelijk en te allen tijde, in te trekken, en instrumenten ontwikkelen om te kunnen ingaan op verzoeken om gegevensoverdraagbaarheid.

171. De informatie kan worden verstrekt bij de ondertekening van de overeenkomst.

3.4.5 Ontvangers

172. In geval van aangifte van diefstal kunnen de locatiegegevens worden doorgegeven aan i) erkende functionarissen van het platform voor bewaking op afstand, en ii) aan de wettelijk erkende autoriteiten.

3.4.6 Beveiliging

173. Hier gelden de algemene aanbevelingen. Zie punt 2.7.