
# Retningslinjer 1/2020 om behandling af personoplysninger i forbindelse med opkoblede køretøjer og mobilitetsrelaterede anvendelser

## Version 2.0

## Vedtaget den 9. marts 2021

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

## Versionshistorik

| | | |
|---|---|---|
| Version 2.0 | 9. marts 2021 | Vedtagelse af retningslinjerne efter offentlig høring |
| Version 1.0 | 28. januar 2020 | Vedtagelse af retningslinjerne med henblik på offentlig høring |

# Indholdsfortegnelse

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter "GDPR"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018[1], og

under henvisning til artikel 12 og 22 i Databeskyttelsesrådets forretningsorden,

**VEDTAGET FØLGENDE RETNINGSLINJER**

# 1 INDLEDNING

1. Som et symbol på det 20. århundredes økonomi er bilen et af de masseforbrugsprodukter, der har haft stor betydning for samfundet som helhed. Biler forbindes almindeligvis med begrebet frihed og anses ofte for langt mere end blot et transportmiddel. De repræsenterer et privat område, hvor mennesket kan træffe selvstændige beslutninger, uden at nogen griber ind udefra. I dag, hvor opkoblede biler bliver mere og mere almindelige, svarer denne vision ikke længere til virkeligheden. Køretøjsmonteret konnektivitet udvides hurtigt fra luksusmodellerne og de førende mærker til de mest populære modeller i mellemsegmentet, og bilerne er ved at udvikle sig til massive datahubs. Ikke kun bilerne, men også førerne og passagererne bliver mere og mere opkoblede. Mange af de modeller, der er kommet på markedet i de sidste par år, har faktisk integrerede sensorer og opkoblet køretøjsmonteret udstyr, som indsamler og registrerer motorens ydeevne, førerens kørestil, de besøgte steder og endda førerens øjenbevægelser, puls eller biometriske data for entydigt at identificere en fysisk person[2].

2. Sådan databehandling sker i et komplekst økosystem, som ikke er begrænset til de traditionelle aktører i bilindustrien, men som også præges af fremkomsten af nye aktører, der tilhører den digitale økonomi. Disse nye aktører tilbyder infotainment-tjenester, f.eks. onlinemusik og vej- og trafikinformation, eller kørselsassistancesystemer og -tjenester, f.eks. autopilotsoftware, opdateringer om bilens tilstand, brugsbaseret forsikring eller dynamiske kort. Da bilerne er opkoblet via elektroniske kommunikationsnet, kan vejinfrastrukturforvaltere og telekommunikationsoperatører, der er involveret i processen, også spille en vigtig rolle med hensyn til de potentielle behandlingsaktiviteter, der udføres på førernes og passagerernes personoplysninger.

3. Opkoblede køretøjer genererer desuden stigende mængder data, hvoraf de fleste kan anses for personoplysninger, da de vedrører førere eller passagerer. Selv om de data, der indsamles af en opkoblet bil, ikke er direkte knyttet til et navn, men til bilens tekniske aspekter og komponenter, vedrører de bilens fører eller passagerer. Data vedrørende f.eks. kørestilen eller den tilbagelagte afstand, data vedrørende slid af bilens dele, lokaliseringsdata eller data, der indsamles af kameraer, kan være knyttet til førerens adfærd, og det samme gælder oplysninger om andre personer, der kan befinde sig i bilen, eller

[1] Henvisninger til "medlemsstater" i hele dette dokument skal forstås som henvisninger til "EØS-medlemsstater".
[2] Infografik "Data and the connected car" af Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

personer, der går forbi bilen. Sådanne tekniske data produceres af en fysisk person og gør det muligt for en dataansvarlig eller en anden person at identificere vedkommende direkte eller indirekte. Køretøjet kan betragtes som en terminal, der kan anvendes af forskellige brugere. Som for en personlig computer har denne potentielle pluralitet af brugere derfor ingen betydning for dataenes personlige karakter.

4. I 2016 gennemførte Fédération Internationale de l'Automobile (FIA) en kampagne i Europa med titlen "My Car My Data" for at få en fornemmelse af, hvad europæere mener om opkoblede biler[3]. Den viste, at der var stor interesse for konnektivitet blandt førerne, men den fremhævede også, at der skal udvises forsigtighed med hensyn til brugen af de data, der produceres af køretøjer, og betydningen af at overholde lovgivningen om beskyttelse er personoplysninger. Udfordringen for hver interessent er derfor at indarbejde "beskyttelse af personoplysninger" allerede fra produktdesignfasen og sikre, at bilbrugerne garanteres gennemsigtighed og kontrol for så vidt angår deres personoplysninger i overensstemmelse med betragtning 78 til GDPR. En sådan tilgang hjælper med at øge brugernes tillid og bidrager derved til den langsigtede udvikling af disse teknologier.

## 1.1 Relateret arbejde

5. Opkoblede køretøjer er blevet et vigtigt emne for myndighederne gennem det sidste årti, især inden for de seneste år. Der er offentliggjort forskellige arbejder på nationalt og internationalt plan vedrørende opkoblede køretøjers sikkerhed og databeskyttelse. Disse forskrifter og initiativer har til formål at supplere de eksisterende ramme for databeskyttelse og beskyttelse af privatlivets fred med sektorspecifikke regler eller retningslinjer for fagfolk.

### 1.1.1 Europæiske og internationale initiativer

6. Siden den 31. marts 2018 har et 112-baseret køretøjsmonteret eCall-system været obligatorisk i alle nye typer M1- og N1-køretøjer (personbiler og lette erhvervskøretøjer)[4,5]. I 2006 havde Artikel 29-Gruppen allerede vedtaget et arbejdsdokument om databeskyttelse og beskyttelse af privatlivets fred i forbindelse med eCall-initiativet[6]. Som tidligere nævnt vedtog Artikel 29-Gruppen også en udtalelse i oktober 2017 vedrørende behandling af personoplysninger i forbindelse med kooperative intelligente transportsystemer (C-ITS).

7. I januar 2017 offentliggjorde Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) en undersøgelse om intelligente bilers cybersikkerhed og modstandsdygtighed, hvor det opstillede de følsomme aktiver samt de tilsvarende trusler, risici, afbødningsfaktorer og mulige sikkerhedsforanstaltninger, der kan gennemføres[7]. I september 2017 vedtog konferencen for myndigheder med ansvar for databeskyttelse og privatlivets fred (ICDPPC) en resolution om opkoblede køretøjer[8]. Endelig vedtog den

[3] Kampagnen "My Car My Data", http://www.mycarmydata.eu/.
[4] Det interoperable EU-dækkende eCall-system, https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Europa-Parlamentets og Rådets afgørelse nr. 585/2014/EU af 15. maj 2014 om indførelse af det interoperable EU-dækkende eCall-system (EØS-relevant tekst), https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32014D0585.
[6] Arbejdsdokument om databeskyttelse og beskyttelse af privatlivets fred i forbindelse med eCall-initiativet, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_da.pdf.
[7] "Cyber security and resilience of smart cars", https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
[8] "Resolution on data protection in automated and connected vehicles", https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.

internationale arbejdsgruppe om databeskyttelse inden for telekommunikation (IWGDPT) et arbejdsdokument om opkoblede køretøjer[9] i april 2018.

### 1.1.2 Nationale initiativer iværksat af medlemmer af Det Europæiske Databeskyttelsesråd ("Databeskyttelsesrådet")

8. I januar 2016 offentliggjorde sammenslutningen af tyske føderale og statslige databeskyttelsesmyndigheder og den tyske automobilsammenslutning (VDA) en fælleserklæring om principperne om databeskyttelse i opkoblede og ikke-opkoblede køretøjer[10]. I august 2017 udsendte Det Forenede Kongeriges Centre for Connected and Autonomous Vehicles (CCAV) en vejledning om principperne om cybersikkerhed for opkoblede og automatiserede køretøjer for at øge bevidstheden om spørgsmålet i bilindustrien[11]. I oktober 2017 udsendte den franske databeskyttelsesmyndighed, Commission Nationale de l'Informatique et des Libertés (CNIL), en overholdelsespakke for opkoblede biler, som indeholder vejledning til interessenterne i, hvordan de kan integrere databeskyttelse gennem design og standardindstillinger, så registrerede kan have effektiv kontrol over deres data[12].

## 1.2 Gældende lovgivning

9. Den relevante retlige ramme i EU er GDPR. Den finder anvendelse i alle tilfælde, hvor databehandling i forbindelse med opkoblede køretøjer involverer behandling af personers personoplysninger.

10. Ud over GDPR fastsættes der i direktiv 2002/58/EF som ændret ved direktiv 2009/136/EF ("e-databeskyttelsesdirektivet") **en specifik standard for alle aktører, som ønsker at lagre eller hente oplysninger, der er lagret på en abonnents eller brugers terminaludstyr i Det Europæiske Økonomiske Samarbejdsområde (EØS).**

11. Størstedelen af e-databeskyttelsesdirektivets bestemmelser (artikel 6, 9 osv.) finder kun anvendelse på udbydere af offentligt tilgængelige elektroniske kommunikationstjenester og udbydere af offentlige kommunikationsnet, men e-databeskyttelsesdirektivets artikel 5, stk. 3, er en generel bestemmelse. Den finder ikke kun anvendelse på elektroniske kommunikationstjenester, men på enhver privat eller offentlig enhed, der lagrer eller læser oplysninger på terminaludstyr uanset arten af de data, der lagres eller hentes.

12. Med hensyn til "*terminaludstyr*" er definitionen fastsat i direktiv 2008/63/EF[13]. I artikel 1, litra a), defineres terminaludstyr som *"alt udstyr, der direkte eller indirekte er tilsluttet et offentligt telekommunikationsnets grænseflade med henblik på at transmittere, behandle eller modtage informationer; i begge tilfælde, ved såvel direkte som indirekte tilslutning, kan denne etableres gennem ledning, lysleder eller elektromagnetisk; tilslutningen er indirekte, hvis der er indskudt et apparat mellem terminaludstyr og det offentlige grænsefladenet b) satellitjordstationsudstyr".*

---

[9] "Working paper on connected vehicles", https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
[10] Data protection aspects of using connected and non-connected vehicles, https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] Principles of cyber security for connected and automated vehicles, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] Compliance package for a responsible use of data in connected cars, https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.
[13] Kommissionens direktiv 2008/63/EF af 20. juni 2008 om konkurrence på markederne for teleterminaludstyr (kodificeret udgave) (EØS-relevant tekst), https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX%3A32008L0063.

13. Såfremt ovennævnte kriterier er opfyldt, bør det opkoblede køretøj og den enhed, der er tilsluttet køretøjet, anses for *"terminaludstyr"* (på samme måde som en computer, en smartphone eller et smart-TV), og bestemmelserne i e-databeskyttelsesdirektivets artikel 5, stk. 3, finder anvendelse, hvor det er relevant.

14. Som Databeskyttelsesrådet har anført i sin udtalelse 5/2019 om samspillet mellem e-databeskyttelsesdirektivet og GDPR[14], bestemmer e-databeskyttelsesdirektivets artikel 5, stk. 3, at der som hovedregel og med forbehold af undtagelserne til denne regel nævnt i punkt 17 nedenfor kræves forudgående samtykke til lagring af oplysninger eller til at skaffe adgang til oplysninger, der allerede er lagret, i en abonnents eller brugers terminaludstyr. I det omfang, at de oplysninger, der lagres i slutbrugerens enhed, udgør personoplysninger, har artikel 5, stk. 3, i e-databeskyttelsesdirektivet forrang for artikel 6 i GDPR med hensyn til lagring eller adgang til disse oplysninger[15]. Enhver behandling af personoplysninger, der sker efter ovennævnte behandlingsaktiviteter, herunder behandling af personoplysninger, der er indhentet gennem adgang til oplysninger på terminaludstyret, skal have et retsgrundlag i henhold til artikel 6 i GDPR for at være lovlig[16].

15. Eftersom den dataansvarlige, når denne anmoder om samtykke til lagring eller adgang til oplysninger i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, skal oplyse den registrerede om formålet med behandlingen — herunder enhver behandling efter ovennævnte aktiviteter (dvs. "senere behandling") — vil samtykke i henhold til artikel 6 i GDPR generelt være det mest hensigtsmæssige retsgrundlag til at dække behandlingen af personoplysninger efter sådanne aktiviteter (for så vidt som formålet med den senere behandling er omfattet af den registreredes samtykke, se punkt 53-54 nedenfor). Samtykke vil derfor sandsynligvis udgøre retsgrundlaget for både lagringen af og adgangen til de oplysninger, der allerede er lagret, og den senere behandling af personoplysninger[17]. Når overholdelsen af artikel 6 i GDPR vurderes, bør der tages hensyn til, at behandlingen som helhed indebærer specifikke aktiviteter, for hvilke EU-lovgiveren har søgt at skabe yderligere beskyttelse[18]. Dataansvarlige skal endvidere tage hensyn til indvirkningen på de registreredes rettigheder, når de fastlægger det passende retsgrundlag, med henblik på at respektere princippet om rimelighed[19]. Artikel 6 i GDPR kan således ikke anvendes af dataansvarlige til at reducere den yderligere beskyttelse, der er fastsat ved e-databeskyttelsesdirektivets artikel 5, stk. 3.

16. Databeskyttelsesrådet minder om, at samtykkebegrebet i e-databeskyttelsesdirektivet er samtykkebegrebet i GDPR og skal opfylde alle krav til samtykke fastsat ved artikel 4, stk. 11, og artikel 7 i GDPR.

17. Mens samtykke er princippet, tillader e-databeskyttelsesdirektivets artikel 5, stk. 3, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i terminaludstyr, undtages fra kravet om informeret samtykke, hvis et af følgende kriterier er opfyldt:

---

[14] Det Europæiske Databeskyttelsesråd, Udtalelse nr. 5/2019 om samspillet mellem e-databeskyttelsesdirektivet og GDPR, navnlig med hensyn til databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser, vedtaget den 12. marts 2019 ("udtalelse 5/2019"), punkt 40.

[15] Ibid., punkt 40.

[16] Ibid., punkt 41.

[17] Samtykke som krævet i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, og samtykke, der kræves som retsgrundlag for behandlingen af data (artikel 6 i GDPR), til det samme specifikke formål kan indhentes samtidig (f.eks. ved at markere et felt, der tydeligt angiver, hvad den registrerede giver samtykke til).

[18] Udtalelse nr. 5/2019, punkt 41.

[19] Det Europæiske Databeskyttelsesråd, Retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i GDPR i forbindelse med leveringen af onlinetjenester til registrerede, version 2.0, 8. oktober 2019, punkt 1.

- **Undtagelse 1:** hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet
- **Undtagelse 2:** hvis det er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.

18. I sådanne tilfælde er behandlingen af personoplysninger, herunder personoplysninger, der er indhentet gennem adgang til oplysninger på terminaludstyret, baseret på et af retsgrundlagene fastsat i artikel 6 i GDPR. Samtykke er f.eks. ikke påkrævet, når databehandling er nødvendig for at levere GPS-navigationstjenester, som den registrerede har anmodet om, når sådanne tjenester kan betegnes som informationssamfundets tjenester.

## 1.3 Anvendelsesområde

19. Databeskyttelsesrådet påpeger, at disse retningslinjer har til formål at fremme overholdelsen i forbindelse med behandling af personoplysninger, der udføres af en lang række interessenter på dette område. De har dog ikke til formål at dække alle de mulige anvendelser i denne sammenhæng eller give retningslinjer for hver tænkelig specifik situation.

20. Dette dokuments anvendelsesområde omfatter navnlig behandlingen af personoplysninger i forbindelse med registreredes ikke-erhvervsmæssige brug af opkoblede køretøjer, dvs. førere, passagerer, køretøjsejere, andre trafikanter osv. Det omhandler mere specifikt de personoplysninger, der: i) behandles i køretøjet, ii) udveksles mellem køretøjet og de personlige enheder, det er tilsluttet (f.eks. brugerens smartphone) eller iii) indsamles lokalt i køretøjet og eksporteres til eksterne enheder (f.eks. køretøjsproducenter, infrastrukturforvaltere, forsikringsselskaber og værksteder) til yderligere behandling.

21. Definitionen af opkoblet køretøj skal forstås bredt i dette dokument. Det kan defineres som et køretøj, der er udstyret med mange elektroniske styreenheder (ECU'er), der er forbundet via et køretøjsmonteret net og konnektivitetsfunktioner, der sætter det i stand til at dele oplysninger med andre enheder både i og uden for køretøjet. Data kan således udveksles mellem køretøjet og personlige enheder, der er tilsluttet det, så det f.eks. er muligt at spejle mobilapplikationer til den informations- og underholdningsenhed, der er indbygget i bilens instrumentbræt. Udviklingen af enkeltstående mobilapplikationer (dvs. applikationer, der er uafhængige af køretøjet, og f.eks. alene kræver anvendelse af en smartphone), der assisterer førere, er omfattet af dette dokument, da de bidraget til køretøjets konnektivitet, selv om de ikke reelt er afhængige af overførslen af data til og fra køretøjet. Der findes mange og forskelligartede applikationer til opkoblede køretøjer, herunder[20]:

22. *Mobilitetsstyring:* funktioner, der sætter førerne i stand til hurtigt og omkostningseffektivt at nå en destination ved at give aktuelle oplysninger om GPS-navigation, potentielt farlige miljøforhold (f.eks. glatte veje), trafiktæthed eller vejarbejde, oplysninger om parkeringsmuligheder eller værksteder, optimalt brændstofforbrug eller vejafgifter.

23. *Køretøjsstyring:* funktioner, der kan hjælpe førerne med at reducere driftsomkostningerne og forbedre brugervenligheden, f.eks. meddelelser om køretøjets tilstand og påmindelser om service, overførsel af brugsdata (f.eks. til værkstedet), tilpassede kørselsafhængige forsikringer, styring af fjernbetjening (f.eks. opvarmningssystemet) eller profilkonfigurationer (f.eks. sædeposition).

24. *Trafiksikkerhed:* funktioner, der advarer føreren om eksterne farer og interne reaktioner, f.eks. kollisionsbeskyttelse, fareadvarsler, vognbaneskiftalarmer, registrering af træthed hos

[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.

føreren, nødopkald (eCall) eller sorte bokse til undersøgelse af sammenstød (system til registrering af data vedrørende hændelser).

25. *Underholdning:* funktioner, der leverer oplysninger til og indebærer underholdning af føreren og passagererne, f.eks. grænseflader til smartphone (håndfrie telefonopkald og stemmegenererede tekstbeskeder), WLAN-hotspots, musik, video, internet, sociale medier, mobilkontor eller tjenester til intelligente huse.

26. *Førerbistand:* funktioner, der medvirker til helt eller delvist automatiseret kørsel, f.eks. kørevejledning eller autopilot i tung trafik, ved parkering eller på motorveje.

27. *Velfærd:* funktioner, der overvåger førerens komfort, kapacitet og evne til at køre, f.eks. registrering af træthed eller tilkald af lægehjælp.

28. Køretøjer kan derfor være opkoblet fra start, og personoplysninger kan indsamles gennem flere kanaler, herunder: i) køretøjssensorer, ii) telematikbokse eller iii) mobilapplikationer (som f.eks. åbnes fra en enhed, der tilhører en fører). For at være omfattet af dette dokuments anvendelsesområde skal mobilapplikationerne være knyttet til selve kørslen. GPS-navigationsapplikationer er f.eks. omfattet. Applikationer, hvis funktioner kun viser førerne steder af interesse (restauranter, historiske monumenter osv.), er imidlertid ikke omfattet af disse retningslinjers anvendelsesområde.

29. En stor del af de data, der genereres af et opkoblet køretøj, vedrører en fysisk person, som er identificeret eller kan identificeres, og udgør derfor personoplysninger. Data omfatter direkte identificerbare data (f.eks. førerens fulde identitet) samt indirekte identificerbare data, f.eks. data om de kørte ture, data om køretøjsbrugen (f.eks. data vedrørende kørestil eller tilbagelagt afstand), eller køretøjets tekniske data (f.eks. data vedrørende slid af køretøjsdele), som kan relateres til en fysisk person gennem krydshenvisning til andre dokumenter og navnlig køretøjets identifikationsnummer (VIN). Personoplysninger i opkoblede køretøjer kan også omfatte metadata, f.eks. køretøjets vedligeholdelsesstatus. Alle data, der kan forbindes med en fysisk person, er med andre ord omfattet af dette dokuments anvendelsesområde.

30. Økosystemet for opkoblede køretøjer omfatter en bredt vifte af interessenter. Dette økosystem omfatter mere præcist de traditionelle aktører i bilindustrien og nye aktører fra den digitale industri. Disse retningslinjer er derfor rettet til bilfabrikanter, udstyrsfabrikanter og leverandører til bilindustrien, værksteder, bilforhandlere, tjenesteudbydere, flådeforvaltere, bilforsikringsselskaber, underholdningsleverandører, telekommunikationsoperatører, vejinfrastrukturforvaltere og offentlige myndigheder samt registrerede. Databeskyttelsesrådet understreger, at kategorierne af registrerede varierer fra den ene tjeneste til den anden (f.eks. førere, ejere, passagerer osv.). Dette er en ikke-udtømmende liste, da økosystemet omfatter et bredt spektrum af tjenester, herunder tjenester, hvor der kræves direkte autentifikation eller identifikation, og tjenester, hvor dette ikke kræves.

31. Nogle databehandlingsaktiviteter, der udføres af fysiske personer i køretøjet, foretages "*som led i rent personlige eller familiemæssige aktiviteter*" og er derfor ikke omfattet af anvendelsesområdet for GDPR[21]. Dette vedrører navnlig brugen af personoplysninger i køretøjet af den ene registrerede, som har indtastet sådanne data i køretøjets instrumentbræt. Databeskyttelsesrådet minder imidlertid om, at GDPR ifølge dens betragtning 18 gælder "*for dataansvarlige eller databehandlere, som tilvejebringer midlerne til behandling af personoplysninger til sådanne personlige eller familiemæssige aktiviteter*".

[21] Se artikel 2, stk. 2, litra c), i GDPR.

### 1.3.1 Uden for dette dokuments anvendelsesområde

32. Arbejdsgivere, der stiller virksomhedens biler til rådighed for personalet, kan ønske at overvåge medarbejdernes aktiviteter (f.eks. for at sikre medarbejderens, varernes eller køretøjers sikkerhed, tildele ressourcer, registrere og fakturere tjenesteydelser eller kontrollere arbejdstiden). Databehandling, der foretages af arbejdsgivere i denne sammenhæng, giver anledning til specifikke overvejelser i forbindelse med ansættelsesforholdet, som kan være omfattet af den nationale arbejdsret, som ikke kan behandles i detaljer i disse retningslinjer[22].

33. Mens databehandling, der foretages i forbindelse med erhvervskøretøjer, der anvendes til professionelle formål (f.eks. offentlig transport), delt transport og MaaS-løsninger, kan give anledning til specifikke overvejelser, som ikke er omfattet af disse generelle retningslinjers anvendelsesområde, finder mange af de principper og anbefalinger, der er anført her, også anvendelse på de typer behandling.

34. Som opkoblede køretøjer, dvs. radioaktiverede systemer, kan de spores passivt, f.eks. ved hjælp af Wi-Fi eller Bluetooth. De adskiller sig i den forstand ikke fra andre opkoblede enheder og er omfattet af e-databeskyttelsesdirektivet, som er under revision. Dette udelukker derfor, at et tæt net af tilstedeværende personer, der anvender de samme smartphone-lokaliseringstjenester, kan foretage omfattende sporing af køretøjer med indbygget Wi-Fi[23]. De rapporterer rutinemæssigt alle synlige Wi-Fi-net til centrale servere. Da indbygget Wi-Fi kan anses for en sekundær køretøjsidentifikator[24], indebærer dette en risiko for en systematisk løbende indsamling af komplette profiler over køretøjsbevægelser.

35. Flere og flere køretøjer udstyres med billedoptagelsesudstyr (f.eks. parkeringskameraer og dashcams). Dette omhandler spørgsmålet om optagelser på offentlige steder, som kræver en vurdering af den relevante lovgivningsramme, som er specifik for hver medlemsstat, er sådan databehandling ikke omfattet af disse retningslinjers anvendelsesområde.

36. Behandlingen af data, der ligger til grund for kooperative intelligente transportsystemer (C-ITS) — som defineret i direktiv 2010/40/EU[25] — er omhandlet i en særlig udtalelse fra Artikel 29-Gruppen[26]. Mens direktivets definition af C-ITS-konceptet ikke omfatter tekniske specifikationer, omhandler Artikel 29-Gruppens udtalelse navnlig kortdistancekommunikation, dvs. kommunikation uden indgriben fra en netoperatør. Den analyserer nærmere specifikke anvendelsesfunktioner til indledende anvendelse og forpligter sig til senere at vurdere de nye problemstillinger, der uden tvivl vil opstå, når en højere automatiseringsgrad er gennemført. Da databeskyttelseskonsekvenserne i forbindelse med C-ITS er meget specifikke (hidtil usete mængder lokaliseringsdata, kontinuerlig transmission af personoplysninger, udveksling af data mellem køretøjer og andre vejinfrastrukturfaciliteter osv.) og stadig drøftes på europæisk plan, er behandlingen af personoplysninger i denne sammenhæng ikke omfattet af disse retningslinjer.

---

[22] Artikel 29-Gruppen har uddybet dette i WP249-udtalelse 2/2017 om databehandling på arbejdspladsen; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

[23] Flere oplysninger kan findes i: 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 og 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, Frankrig, 23.-27.7.2017, s. 32-37.

[25] Direktiv 2010/40/EU af 7. juli 2020 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32010L0040.

[26] Artikel 29-Gruppen: Udtalelse 03/2017 om behandling af personoplysninger i forbindelse med kooperative intelligente transportsystemer (C-ITS). http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

37. Endelig har dette dokument ikke til formål at omhandle alle mulige problemstillinger og spørgsmål, som opkoblede køretøjer giver anledning til, og kan derfor ikke anses for udtømmende.

## 1.4 Definitioner

38. **Behandling** af personoplysninger omfatter enhver aktivitet, der involverer personoplysninger, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse[27].

39. Den **registrerede** er den fysiske person, som de data, der er omfattet af behandlingen, vedrører. I forbindelse med opkoblede køretøjer kan det navnlig være føreren (primær eller lejlighedsvis), passagererne eller køretøjets ejer[28].

40. Den **dataansvarlige** er den person, der afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling i opkoblede køretøjer[29]. Dataansvarlige kan omfatte tjenesteudbydere, der behandler køretøjsdata med henblik på at sende trafikoplysninger, meddelelser om miljøvenlig kørsel eller advarsler vedrørende køretøjets funktion til føreren, forsikringsselskaber, der tilbyder kørselsafhængige forsikringer, eller bilfabrikanter, der indsamler data om slid, som påvirker køretøjets dele, med henblik på at forbedre kvaliteten. I henhold til artikel 26 i GDPR kan to eller flere dataansvarlige i fællesskab fastlægge formålene med og hjælpemidlerne til behandling og dermed anses for fælles dataansvarlige. I dette tilfælde skal de klart definere deres respektive forpligtelser, navnlig med hensyn til udøvelsen af registreredes rettigheder og levering af oplysninger som omhandlet i artikel 13 og 14 i GDPR.

41. **databehandler** er enhver person, der behandler personoplysninger på den dataansvarliges vegne[30]. Databehandleren indsamler og behandler data efter anvisning fra den dataansvarlige uden at anvende disse data til sine egne formål. I en række tilfælde behandler udstyrsfabrikanter og leverandører til bilindustrien f.eks. data på vegne af bilfabrikanter (hvilket ikke indebærer, at de ikke kan være dataansvarlige i andre forbindelser). Ud over et krav om, at databehandlere gennemfører passende tekniske og organisatoriske foranstaltninger for at garantere et sikkerhedsniveau, der står i forhold til risikoen, fastsætter artikel 28 i GDPR databehandlerens øvrige forpligtelser.

42. **Modtageren** er fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, uanset om det er en tredjemand eller ej[31]. En handelspartner, der modtager personoplysninger, der er genereret fra køretøjet, af tjenesteudbyderen, er en modtager af personoplysninger. Uanset om de optræder som en ny dataansvarlig eller som en databehandler, skal de opfylde alle de forpligtelser, der følger af GDPR.

43. Offentlige myndigheder, som vil kunne få meddelt personoplysninger som led i en isoleret forespørgsel i henhold til EU-retten eller medlemsstaternes nationale ret, anses dog ikke for modtagere[32]. De offentlige myndigheders behandling af disse oplysninger skal overholde de gældende databeskyttelsesregler afhængigt af formålet med behandlingen.

---

[27] Se artikel 4, nr. 2), i GDPR.
[28] Se artikel 4, nr. 1), i GDPR.
[29] Artikel 4, nr. 7), i GDPR og Det Europæiske Databeskyttelsesråd, Retningslinjer 7/2020 om begreberne dataansvarlig og databehandler i databeskyttelsesforordningen. ("retningslinjer 7/2020").
[30] Se artikel 4, nr. 8), i GDPR og retningslinjer 7/2020.
[31] Se artikel 4, nr. 9), i GDPR og retningslinjer 7/2020.
[32] Artikel 4, nr. 9), i GDPR og betragtning 31 til samme forordning.

Retshåndhævende myndigheder er f.eks. autoriserede tredjeparter, når de anmoder om personoplysninger som led en undersøgelse i henhold til EU-retten eller national ret.

## 1.5 Risici for beskyttelse af privatlivets fred og databeskyttelse

44. Artikel 29-Gruppen har allerede ved flere lejligheder udtrykt bekymring over systemer vedrørende tingenes internet (IoT), som også er relevante for opkoblede køretøjer[33]. Problemerne i forbindelse med datasikkerhed og kontrol, der allerede er fremhævet i forbindelse med IoT, er endnu mere følsomme i forbindelse med opkoblede køretøjer, da de omfatter betænkeligheder vedrørende trafiksikkerheden — og kan påvirke førerens fysiske integritet — i et miljø, der traditionelt opfattes som isoleret og beskyttet mod indgriben udefra.

45. Opkoblede køretøjer giver endvidere anledning til betydelige bekymringer vedrørende databeskyttelse og beskyttelse af privatlivets fred i forbindelse med behandlingen af lokaliseringsdata, da den stadig mere indgribende karakter heraf kan påvirke de nuværende muligheder for at forblive anonym. Databeskyttelsesrådet ønsker at lægge særligt vægt på og styrke interessenternes bevidsthed om det forhold, at anvendelsen af lokaliseringsteknologier kræver, at der gennemføres specifikke sikkerhedsforanstaltninger for at forhindre overvågning af personer og misbrug af disse data.

### 1.5.1 Mangel på kontrol og informationsasymmetri

46. Køretøjsførere og -passagerer informeres muligvis ikke altid tilstrækkeligt om den behandling af data, der foretages i eller gennem et opkoblet køretøj. Oplysningerne gives f.eks. kun til køretøjets ejer, som ikke nødvendigvis er føreren, og gives måske heller ikke inden for en relevant tidshorisont. Der er derfor risiko for, at de berørte personer tilbydes utilstrækkelige funktioner til eller mulighed for at udøve den kontrol, der er nødvendig for, at de kan påberåbe sig deres ret til beskyttelse af personoplysninger og retten til privatlivets fred. Dette punkt er vigtigt, eftersom køretøjer i løbet af deres levetid kan tilhøre mere end én ejer, enten fordi de sælges, eller fordi de er leaset og ikke købt.

47. Kommunikation i køretøjet kan desuden udløses automatisk og som standard, uden at personen er klar over det. Når det ikke er muligt effektivt at kontrollere, hvordan køretøjet og dets opkoblede udstyr interagerer, må det nødvendigvis være usædvanligt vanskeligt for brugeren at kontrollere datastrømmen. Det vil være endnu vanskeligere at kontrollere den senere anvendelse heraf og forhindre et potentielt funktionsskred.

### 1.5.2 Kvaliteten af brugerens samtykke

48. Databeskyttelsesrådet understreger, at alle elementer af et gyldigt samtykke — når databehandlingen er baseret på samtykke — skal være opfyldt, dvs. at samtykket skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede som fortolket i Databeskyttelsesrådets retningslinjer for samtykke[34]. Dataansvarlige skal være meget opmærksomme på reglerne for at indhente gyldigt tilsagn fra forskellige deltagere, f.eks. bilejere eller bilbrugere. Et sådant samtykke skal gives særskilt til forskellige formål og må ikke være sammenknyttet med kontrakten om køb eller leasing af en ny bil. Det skal være lige så nemt at tilbagetrække samtykket som at give det.

49. Det samme gør sig gældende, hvis der kræves samtykke for at overholde e-databeskyttelsesdirektivet, f.eks. hvis oplysninger lagres, eller der opnås adgang til oplysninger, der allerede er lagret, i køretøjet, som det i visse tilfælde kræves i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3. Som anført ovenfor skal samtykke i denne sammenhæng fortolkes i henhold til GDPR.

50. I mange tilfælde er brugeren ikke opmærksom på den databehandling, der foretages i vedkommendes køretøj. En sådan mangel på information udgør en betydelig hindring for at

[33] Artikel 29-Gruppen — Udtalelse 8/2014 om den seneste udvikling inden for tingenes internet, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_da.pdf.
[34] Det Europæiske Databeskyttelsesråd, Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020 ("retningslinjer 5/2020").

påvise gyldigt samtykke i henhold til GDPR, da samtykket skal være informeret. Under sådanne omstændigheder kan samtykke ikke bruges som retsgrundlag for den tilsvarende databehandling i henhold til GDPR.

51. De mekanismer, der sædvanligvis anvendes til at indhente personers samtykke, kan være vanskelige at anvende i forbindelse med opkoblede køretøjer, og det fører til et samtykke af "lav kvalitet", som er baseret på mangel på information eller reel manglende mulighed for give et tilpasset samtykke i overensstemmelse med de præferencer, der tilkendegives af personer. Det kan i praksis være vanskeligt at indhente samtykke fra førere og passagerer, der ikke har forbindelse med køretøjets ejer, når der er tale om brugte, leasede, lejede eller lånte køretøjer.

52. Hvis e-databeskyttelsesdirektivet ikke kræver den registreredes samtykke, har den dataansvarlige imidlertid mulighed for at vælge det retsgrundlag i henhold til artikel 6 i GDPR, der er mest hensigtsmæssigt for den pågældende behandling af personoplysninger.

### 1.5.3 Viderebehandling af personoplysninger

53. Når data indsamles på grundlag af samtykke som krævet i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, eller på grundlag af en af undtagelserne i artikel 5, stk. 3, og efterfølgende behandles i henhold til artikel 6 i GDPR, må de kun viderebehandles, hvis den dataansvarlige indhenter yderligere samtykke til dette andet formål, eller hvis den dataansvarlige kan godtgøre, at dette er baseret på EU-retten eller en medlemsstats nationale ret af hensyn til de mål, der er omhandlet i artikel 23, stk. 1, i GDPR[35]. Databeskyttelsesrådet finder, at viderebehandling på grundlag af en forenelighedstest i overensstemmelse med artikel 6, stk. 4, i GDPR ikke er tilladt i sådanne tilfælde, da det ville undergrave e-databeskyttelsesdirektivets standard for databeskyttelse. Samtykke skal, når det er påkrævet i henhold til e-databeskyttelsesdirektivet, være specifikt og informeret, dvs. at de registrerede skal være vidende om hvert databehandlingsformål og have ret til at afvise specifikke tilfælde[36]. Hvis viderebehandling på grundlag af en forenelighedstest i henhold til artikel 6, stk. 4, i GDPR tillades, vil det omgå selve de principper, der ligger til grund for samtykkekravene i det nuværende direktiv.

54. Databeskyttelsesrådet minder om, at det indledende samtykke aldrig kan legitimere viderebehandling, da samtykke skal være informeret og specifikt for at være gyldigt.

55. Telemetridata, der indsamles under brugen af køretøjet til vedligeholdelsesmæssige formål, må f.eks. ikke videregives til bilforsikringsselskaber uden brugerens samtykke til formålet om at oprette førerprofiler for at tilbyde forsikringspolicer baseret på føreradfærd.

56. Data, der indsamles af opkoblede køretøjer, må endvidere kun behandles af retshåndhævende myndigheder for at registrere hastighedsovertrædelser eller andre overtrædelser, hvis og når de specifikke betingelser i direktivet om retshåndhævelse er opfyldt. I dette tilfælde anses sådanne data for at vedrørende straffedomme og lovovertrædelser på de betingelser, der er fastsat i artikel 10 i GDPR og eventuelt gældende national lovgivning. Fabrikanter kan udlevere sådanne data til de retshåndhævende myndigheder, hvis de specifikke betingelser for sådan behandling er opfyldt. Databeskyttelsesrådet påpeger, at behandling af personoplysninger alene med henblik på at imødekomme anmodninger fra retshåndhævende myndigheder ikke udgør et specifikt, udtrykkeligt og legitimt formål i den forstand, der er fastsat i artikel 5, stk. 1, litra b), i GDPR. Hvis retshåndhævende myndigheder har sådanne beføjelser i henhold til loven, kan de være en tredjemand som defineret i artikel 4, nr. 10), i GDPR, og fabrikanterne kan da give dem

[35] Se også Det Europæiske Databeskyttelsesråd, "Guidelines 10/2020 on restrictions under Article 23 GDPR".
[36] Retningslinjer 5/2020, afsnit 3.2 og 3.3.

alle data, de har til rådighed, i overensstemmelse med den relevante retlige ramme i hver medlemsstat.

### 1.5.4 Overdreven indsamling af data

57. Med det stadigt stigende antal sensorer, der monteres i opkoblede køretøjer, er der en meget høj risiko for overdreven indsamling af data i forhold til, hvad der er nødvendigt for at opfylde formålet.

58. Udviklingen af nye funktioner og mere specifikt funktioner, der er baseret på maskinlæringsalgoritmer, kan kræve, at der indsamles store mængder data over en lang periode.

### 1.5.5 Personoplysningssikkerhed

59. De mange forskellige funktioner, tjenester og grænseflader (f.eks. web, USB, RFID og Wi-Fi), der findes i opkoblede køretøjer, øger angrebsoverfladen og dermed antallet af potentielle sårbarheder, hvorigennem personoplysninger kan kompromitteres. I modsætning til de fleste IoT-enheder er opkoblede køretøjer kritiske systemer, hvor et brud på sikkerheden kan bringe brugernes og de omkringværende personers liv i fare. Betydningen af at imødegå risikoen for, at hackere forsøger at udnytte opkoblede køretøjers svagheder, øges dermed.

60. Personoplysninger, der lagres i køretøjer og/eller på eksterne steder (f.eks. i cloud computing-infrastrukturer), skal desuden være tilstrækkelig beskyttet mod uautoriseret adgang. Ved vedligeholdelse skal et køretøj f.eks. afleveres til en tekniker, som skal have adgang til nogle af køretøjets tekniske data. Teknikeren skal have adgang til de tekniske data, men teknikeren kan f.eks. også forsøge at få adgang til alle data, der er lagret i køretøjet.

# 2 GENERELLE ANBEFALINGER

61. For at afbøde de risici for registrerede, der er omhandlet ovenfor, bør køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre interessenter, der kan fungere som dataansvarlig eller databehandler i forbindelse med opkoblede køretøjer, følge nedenstående generelle anbefalinger.

## 2.1 Kategorier af data

62. Som anført i indledningen anses de fleste data, der er forbundet med opkoblede køretøjer, for personoplysninger, for så vidt som de kan knyttes til en eller flere identificerbare personer. Dette omfatter tekniske data vedrørende køretøjets bevægelser (f.eks. hastighed og tilbagelagt afstand) og vedrørende køretøjets tilstand (f.eks. kølevæsketemperatur, omdrejningstal og dæktryk). Visse data, der genereres af opkoblede køretøjer, kræver særlig opmærksomhed i medfør af deres følsomhed og/eller potentielle indvirkning på de registreredes rettigheder og interesser. På nuværende tidspunkt har Databeskyttelsesrådet opstillet tre kategorier af personoplysninger, der kræver særlig opmærksomhed fra køretøjs- og udstyrsfabrikanters, tjenesteudbyderes og andre dataansvarliges side: lokaliseringsdata, biometriske data (og særlige kategorier af personoplysninger behandles, jf. artikel 9 i GDPR) og data, der kan afsløre lovovertrædelser eller trafikforseelser.

### 2.1.1 Lokaliseringsdata

63. Når køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre dataansvarlige indsamler personoplysninger, bør de være opmærksomme på, at lokaliseringsdata er særligt afslørende med hensyn til de registreredes vaner. De ruter, som en registreret kører, er meget karakteristiske, idet de gør det mulig at udlede vedkommendes arbejdssted og bopæl samt en førers interesseområder (fritid), og de kan muligvis afsløre følsomme oplysninger som f.eks. religion via de religiøse steder, vedkommende besøger, eller seksuel orientering via de steder, vedkommende besøger. Køretøjs- og udstyrsfabrikanten, tjenesteudbyderen

eller en anden dataansvarlig bør derfor være særligt omhyggelige med ikke at indsamle lokaliseringsdata, medmindre dette er strengt nødvendigt til behandlingen. Når behandlingen f.eks. består i at registrere køretøjets bevægelse, kan et gyroskop udføre denne funktion, uden at der er behov for at indsamle lokaliseringsdata.

64. Generelt skal følgende principper også overholdes ved indsamling af lokaliseringsdata:

- Hyppigheden af adgangen til og detaljeringsgraden af de indsamlede lokaliseringsdata skal konfigureres i forhold til formålet med behandlingen. En vejrapplikation bør f.eks. ikke kunne få adgang til køretøjets position hvert sekund, heller ikke med den registreredes samtykke.
- Brugeren gives nøjagtig information om formålet med behandlingen (f.eks. lagres lokaliseringshistorikken? Hvis ja, til hvilket formål?).
- Der indhentes et gyldigt samtykke (frit, specifikt og informeret), som er særskilt i forhold til de generelle betingelser for f.eks. salg eller brug af den køretøjsmonterede computer, når behandlingen er baseret på samtykke.
- Lokaliseringen aktiveres kun, når brugeren benytter en funktion, hvor køretøjets position skal være kendt, og ikke som standard og kontinuerligt, når bilen er startet.
- Brugeren oplyses om, at lokaliseringsfunktionen er blevet aktiveret, f.eks. ved brug af ikoner (f.eks. en pil, der bevæger sig hen over skærmen.
- Lokaliseringsfunktionen skal til enhver kunne deaktiveres.
- Der fastsættes en begrænset lagringsperiode.

### 2.1.2 Biometriske data

65. I forbindelse med opkoblede køretøjer kan biometriske data, der anvendes til entydigt at identificere en fysisk person, behandles i overensstemmelse med artikel 9 i GDPR og de nationale undtagelser til at gøre det muligt at få adgang til et køretøj, til at godkende føreren/ejeren og/eller til at gøre det muligt at få adgang til en førers profilindstillinger og præferencer. Med hensyn til brugen af biometriske data indebærer garantien for, at den registrerede har fuld kontrol over sine data, på den ene side, at der kan anvendes et ikkebiometrisk alternativ (f.eks. en fysisk nøgle eller en kode) uden yderligere begrænsninger (dvs. at brugen af biometri ikke bør være påkrævet), og på den anden side, at den biometriske skabelon kun lagres og sammenlignes lokalt i krypteret form, således at biometriske data ikke behandles af en ekstern læsnings-/sammenligningsterminal.

66. I forbindelse med biometriske data[37] skal det sikres, at løsningen til biometrisk autentifikation er tilstrækkelig pålidelig og bl.a. overholder følgende principper:

- indstillingen af den biometriske løsning (f.eks. raten af falsk positive resultater og falsk negative resultater) er tilpasset sikkerhedsniveauet i den krævede adgangskontrol
- den anvendte biometriske løsning er baseret på en sensor, der er modstandsdygtig over for angreb (f.eks. brug af fladtrykt print til fingeraftryksgenkendelse)
- antallet af autentifikationsforsøg er begrænset
- den biometriske skabelon/model er lagret i køretøjet i krypteret form ved brug af en kryptografisk algoritme og nøglestyring baseret på den nyeste teknologi
- de rådata, der anvendes til den biometriske skabelon og til brugerautentifikation, behandles i realtid uden at blive lagret, heller ikke lokalt.

[37] Forbuddet i artikel 9, stk. 1, i GDPR vedrører kun "*biometriske data med det formål entydigt at identificere en fysisk person*".

### 2.1.3 Data, der afslører lovovertrædelser eller andre forseelser

67. Med henblik på at behandle data, der vedrører potentielle lovovertrædelser som omhandlet i artikel 10 i GDPR, anbefaler Databeskyttelsesrådet, at der foretages lokal behandling af dataene, hvor den registrerede har fuld kontrol over den pågældende behandling (se betragtningerne om lokal behandling i afsnit 2.4). Med visse undtagelser (se casestudiet om ulykkesundersøgelser i afsnit 3.3) er ekstern behandling af data, der kan afsløre lovovertrædelser eller andre forseelser, faktisk forbudt. Afhængigt af dataenes følsomhed skal der derfor indføres stærke sikkerhedsforanstaltninger, f.eks. de foranstaltninger, der er beskrevet i afsnit 2.7, for at sikre beskyttelse mod ulovlig adgang til, ændring af og sletning af sådanne data.

68. Visse kategorier af personoplysninger fra opkoblede køretøjer kan afsløre, at en lovovertrædelse eller en anden forseelse er blevet eller er ved at blive begået ("overtrædelsesrelaterede data"), og er derfor omfattet af særlige begrænsninger (f.eks. data, der viser, at køretøjet har krydset en fuldt optrukket linje, eller køretøjets øjeblikkelige hastighed kombineret med præcise lokaliseringsdata). Hvis sådanne data behandles af de kompetente nationale myndigheder med henblik på strafferetlig efterforskning og retsforfølgning af en lovovertrædelse, finder forholdsreglerne i artikel 10 i GDPR anvendelse.

## 2.2 Formål

69. Personoplysninger må behandles til forskellige formål i forbindelse med opkoblede køretøjer, herunder førersikkerhed, forsikring, effektiv transport, underholdning eller informationstjenester. I overensstemmelse med GDPR skal dataansvarlige sikre, at deres formål er "specifikt, udtrykkeligt og legitimt", at data ikke behandles på en måde, der er uforenelig med dette formål, og at der er et gyldigt retsgrundlag for behandlingen som krævet i artikel 5 i GDPR. I disse retningslinjers del III gives der konkrete eksempler på formål, der kan forfølges af dataansvarlige med aktiviteter, der involverer opkoblede køretøjer, sammen med specifikke anbefalinger vedrørende hver type behandling.

## 2.3 Relevans og dataminimering

70. For at overholde princippet om dataminimering[38] bør køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre dataansvarlige være særligt opmærksomme på de kategorier af data, de skal bruge fra et opkoblet køretøj, da de kun må indsamle personoplysninger, der er relevante og nødvendige for behandlingen. Lokaliseringsdata er f.eks. særligt indgribende og kan afsløre mange af de registreredes vaner. De økonomiske aktører bør være særligt opmærksomme på ikke at indsamle lokaliseringsdata, medmindre dette er absolut nødvendigt for behandlingen (se betragtningerne om lokaliseringsdata ovenfor i afsnit 2.1).

## 2.4 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

71. Under hensyntagen til mængden og forskelligartetheden af de personoplysninger, der produceres af opkoblede køretøjer, bemærker Databeskyttelsesrådet, at dataansvarlige skal sikre, at de teknologier, der anvendes i forbindelse med opkoblede køretøjer, er konfigureret til at respektere personers privatliv, ved at opfylde forpligtelserne til databeskyttelse gennem design og gennem standardindstillinger, som det kræves i artikel 25 i GDPR. Teknologierne bør være designet til at minimere indsamlingen af personoplysninger, omfatte standardindstillinger, der beskytter privatlivet, og sikre, at registrerede er velinformerede og har mulighed for let at ændre de konfigurationer, der er knyttet til deres personoplysninger. Specifik vejledning om, hvordan fabrikanter og tjenesteudbydere kan opfylde kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, kan være nyttige for industrien og for tredjepartsudbydere af applikationer.

[38] Artikel 5, stk. 1, litra c), i GDPR.

72. En række generelle principper, som er omhandlet nedenfor, kan hjælpe med at afbøde risiciene for fysiske personers rettigheder og frihedsrettigheder i forbindelse med opkoblede køretøjer[39].

### 2.4.1 Lokal behandling af personoplysninger

73. Generelt bør køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre dataansvarlige så vidt muligt anvende processer, der ikke involverer personoplysninger eller overførsel af personoplysninger uden for køretøjet (dvs. oplysningerne behandles internt). Karakteren af opkoblede køretøjer indebærer imidlertid visse risici, f.eks. mulighed for angreb på lokal behandling fra aktører udefra eller for lækage af lokale data gennem salg af dele fra køretøjet. Der kræves derfor tilstrækkelig opmærksomhed og tilstrækkelige sikkerhedsforanstaltninger til at sikre, at den lokale behandling forbliver lokal. Dette scenarie har den fordel, at det garanterer brugeren enekontrol og fuld kontrol over vedkommendes personoplysninger, og det indebærer således "gennem design" færre risici for privatlivets fred, især ved at forbyde enhver databehandling, der foretages af interessenter uden den registreredes viden. Det gør det også muligt at behandle følsomme data, f.eks. biometriske data eller data vedrørende lovovertrædelser eller andre forseelser, samt detaljerede lokaliseringsdata, som ellers er omfattet af strengere regler (se nedenfor). Det indebærer ligeledes færre cybersikkerhedsrisici og begrænset latenstid, som gør det særligt velegnet til automatiserede kørselsassistancefunktioner. Eksempler på løsninger af denne type omfatter:

- applikationer til miljøvenlig kørsel, som behandler data i køretøjet med det formål at vise gode råd om miljøvenlig kørsel i realtid på den køretøjsmonterede skærm
- applikationer, der omfatter overførsel af personoplysninger til en enhed, f.eks. en smartphone, under brugerens fulde kontrol (via f.eks. Bluetooth eller Wi-Fi), og hvor køretøjets data ikke overføres til applikationsudbyderne eller køretøjsfabrikanterne dette omfatter f.eks. tilslutning af en smartphone med henblik på at anvende bilens skærm, multimediesystemer, mikrofon (eller andre sensorer) til telefonopkald osv., for så vidt som de indsamlede data forbliver under den registreredes kontrol og udelukkende anvendes til at levere den tjeneste, vedkommende har anmodet om
- køretøjsmonterede sikkerhedsforbedrende applikationer, f.eks. applikationer, der afgiver lydsignaler eller vibrerer rattet, når en fører overhaler en bil uden at give signal eller overskrider de optrukne linjer, eller som viser advarsler om køretøjets tilstand (f.eks. en advarsel om slid på bremsebelægningerne)
- applikationer til oplåsning, start og/eller aktivering af visse køretøjskommandoer ved brug af førerens biometriske data, som er lagret i køretøjet (f.eks. ansigts- eller stemmemodeller eller fingeraftryksbilleder).

74. Applikationer som de ovennævnte indebærer behandling, der foretages alene med henblik på en fysisk persons udførelse fuldstændigt personlige aktiviteter (dvs. uden overførsel af personoplysninger til en dataansvarlig eller databehandler). I henhold til artikel 2, stk. 2, i GDPR, **falder disse applikationer derfor uden for anvendelsesområdet for GDPR.**

75. GDPR gælder ikke for en fysisk persons behandling af oplysninger under en rent personlig eller familiemæssig aktivitet, men forordningen finder anvendelse på dataansvarlige eller databehandlere, som tilvejebringer midlerne til behandling af personoplysninger til sådanne personlige eller familiemæssige aktiviteter (bilfabrikanter, tjenesteudbydere osv.) i overensstemmelse med betragtning 18 til GDPR. Når de handler som dataansvarlige eller

[39] Se også Det Europæiske Databeskyttelsesråd, Retningslinjer 4/2019 om artikel 25 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, version 2.0, Vedtaget den 20. oktober 2020 ("retningslinjer 4/2019").

databehandlere, skal de derfor udvikle sikre bilapplikationer under behørig hensyntagen til princippet om databeskyttelse gennem design og gennem standardindstillinger. I overensstemmelse med betragtning 78 til GDPR gælder følgende "*Når producenter af produkter, tjenester og applikationer udvikler, designer, udvælger og bruger applikationer, tjenester og produkter, der er baseret på behandling af personoplysninger eller behandler personoplysninger, for at udføre deres opgaver, bør de tilskyndes til at tage højde for retten til databeskyttelse i forbindelse med udvikling og design af sådanne produkter, tjenester og applikationer og til under behørig hensyntagen til det aktuelle tekniske niveau at sørge for, at de dataansvarlige og databehandlerne er i stand til at opfylde deres databeskyttelsesforpligtelser*"[40]. Dette vil på den ene side forbedre udviklingen af brugercentrerede tjenester, og det vil på den anden side lette og sikre enhver videreanvendelse i fremtiden, som kan være omfattet af anvendelsesområdet for GDPR. Databeskyttelsesrådet anbefaler mere specifikt, at der udvikles en sikker applikationsplatform i bilen, som er fysisk adskilt fra de sikkerhedsrelevante bilfunktioner, således at adgangen til bildata ikke er afhængig af unødvendige eksterne cloudfunktioner.

76. Lokal databehandling bør så vidt muligt overvejes af bilfabrikanter og tjenesteudbydere med henblik på at afbøde de potentielle risici i forbindelse med cloud-behandling, som Artikel 29-Gruppen understreger i sin udtalelse om cloud computing[41].

77. Brugerne bør generelt kunne kontrollere den måde, hvorpå deres data indsamles og behandles i køretøjet:

- oplysninger om behandlingen skal gives på førerens sprog (manual, indstillinger osv.)
- Databeskyttelsesrådet anbefaler, at kun data, der er strengt nødvendige for køretøjets funktion, behandles som standard. Registrerede bør have mulighed for at aktivere eller deaktivere databehandlingen for hvert andet formål og hver anden dataansvarlig/-behandler og have mulighed for at slette de pågældende data under hensyntagen til formålet og retsgrundlaget for databehandlingen
- data bør ikke overføres til tredjemand (dvs. brugeren har eneadgang til dataene)
- data bør kun opbevares, så længe det er nødvendigt for at levere tjenesten, eller som det ellers kræves i henhold til EU-retten eller medlemsstatens nationale ret
- registrerede bør permanent kunne slette personoplysninger, inden køretøjet sættes til salg
- registrerede bør så vidt muligt have direkte adgang til data, der genereres af disse applikationer.

78. Eftersom det ikke altid er muligt at foretage lokal databehandling, kan "hybrid behandling" ofte anvendes. I forbindelse med f.eks. anvendelsesbaseret forsikring kan personoplysninger vedrørende kørselsadfærd (f.eks. kraft på bremsepedalen, kørte kilometer osv.) behandles enten i køretøjet eller af telematikudbyderen på vegne af forsikringsselskabet (den dataansvarlige) med henblik på at generere numeriske scorer, der overføres til forsikringsselskabet med faste mellemrum (f.eks. månedligt). På denne måde får forsikringsselskabet ikke adgang til rådata om adfærd, men kun til den samlede score, der er resultatet af behandlingen. Dette sikrer, at principperne om dataminimering opfyldes gennem design. Det betyder også, at brugerne har mulighed for at udøve deres ret, når data er lagret af andre parter: En bruger kan f.eks. slette data, der er lagret i et værksteds eller en forhandlers systemer på de betingelser, der er fastsat i artikel17 i GDPR.

[40] For flere anbefalinger vedrørende databeskyttelse gennem design, se også retningslinjer 4/2019.
[41] Artikel 29-Gruppen — Udtalelse 5/2012 om cloud computing, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_da.pdf.

### 2.4.2 Anonymisering og pseudonymisering

79. Hvis det forventes, at personoplysninger vil blive overført uden for køretøjet, bør det overvejes at anonymisere dem, inden de overføres. Ved anonymiseringen bør den dataansvarlige tage hensyn til alle involverede behandlingsaktiviteter, som potentielt kan føre til genidentifikation af data, f.eks. overførsel af lokalt anonymiserede data. Databeskyttelsesrådet minder om, at principperne om databeskyttelse ikke gælder for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres[42]. Når et datasæt er fuldt anonymiseret, og personer ikke længere kan identificeres, finder den europæiske databeskyttelsesret ikke længere anvendelse. Følgelig kan anonymisering, hvor det er relevant, være en god strategi for at bevare fordelene og afbøde risiciene ved opkoblede køretøjer.

80. Som anført i Artikel 29-Gruppens udtalelse om anonymiseringsteknikker kan der anvendes forskellige metoder — nogle gange i kombination — til at opnå dataanonymisering[43].

81. Andre teknikker, f.eks. pseudonymisering[44], kan hjælpe med at minimere de risici, der genereres af databehandlingen, under hensyntagen til, at det i de fleste tilfælde ikke er nødvendigt med direkte identificerbare data til at opfylde formålene med behandlingen. Pseudonymisering forbedrer, hvis den understøttes af sikkerhedsforanstaltninger, beskyttelsen af personoplysninger ved at mindske risiciene for misbrug. Pseudonymisering er i modsætning til anonymisering reversibel, og pseudonymiserede data anses for personoplysninger ifølge GDPR.

### 2.4.3 Konsekvensanalyse af databeskyttelse

82. I betragtning af omfanget og følsomheden af de personoplysninger, der kan genereres *via* opkoblede køretøjer, er det sandsynligt, at behandling — navnlig i situationer, hvor personoplysninger behandles uden for køretøjet — ofte vil medføre en høj risiko for personers rettigheder og frihedsrettigheder. Hvis dette er tilfældet, skal de økonomiske aktører foretage en konsekvensanalyse vedrørende databeskyttelse med henblik på at identificere og afbøde risiciene som omhandlet i artikel 35 og 36 i GDPR. Selv hvis en konsekvensanalyse vedrørende databeskyttelse ikke er påkrævet, er det bedste praksis at gennemføre en sådan analyse så tidligt i designprocessen som muligt. Derved kan de økonomiske aktører tage hensyn til resultaterne af denne analyse i deres designvalg inden udrulningen af nye teknologier.

## 2.5 Oplysning

83. Inden behandlingen af personoplysninger skal den registrerede oplyses om den dataansvarliges identitet (f.eks. køretøjs- og udstyrsfabrikanten eller tjenesteudbyderen), formålet med behandlingen, datamodtagerne, det tidsrum, hvor personoplysningerne vil blive opbevaret, og den registreredes rettigheder i henhold til GDPR[45].

84. Køretøjs- og udstyrsfabrikanten, tjenesteudbyderen eller en anden dataansvarlig bør desuden give den registrerede følgende oplysninger på en klar, enkel og lettilgængelig måde:

---

[42] Artikel 4, nr. 1), i GDPR og betragtning 26 til samme forordning.
[43] Artikel 29-Gruppen — Udtalelse 05/2014 om anonymiseringsteknikker, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf.
[44] Artikel 4, nr. 5), i GDPR. Enisa-rapport af 3.12.2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] Artikel 5, stk. 1, litra a), og artikel 13 i GDPR. Se også Artikel 29-Gruppen, Retningslinjer for gennemsigtighed i henhold til forordning 2016/679 (wp260rev.01), godkendt af Databeskyttelsesrådet.

- kontaktoplysninger for databeskyttelsesrådgiveren
- formålene med den behandling, som personoplysningerne skal bruges til, samt retsgrundlaget for behandlingen
- en udtrykkelig angivelse af de legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis sådanne legitime interesser er retsgrundlaget for behandlingen
- eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
- retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede eller til at gøre indsigelse mod behandling samt retten til dataportabilitet
- retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf, hvis behandlingen er baseret på samtykke
- hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation, og de garantier, der anvendes ved overførslen
- om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger
- forekomsten af automatiske afgørelser, herunder profilering, som har retsvirkning eller på tilsvarende vis påvirker den registrerede væsentligt, og meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede. Dette kan navnlig være tilfældet ved leveringen af brugsbaseret forsikring til personer
- retten til at indgive en klage til en tilsynsmyndighed
- information om viderebehandling
- klare og udførlige oplysninger om hver dataansvarlig, hvis der er tale om fælles dataansvar.

85. I nogle tilfælde indsamles personoplysninger ikke direkte fra den berørte person. En køretøjs- og udstyrsfabrikant kan f.eks. få en forhandler til at indsamle oplysninger om køretøjets ejer med henblik på at tilbyde vejhjælpstjenester. Hvis data ikke indsamles direkte, skal køretøjs- og udstyrsfabrikanten, tjenesteudbyderen eller en anden dataansvarlig i tillæg til ovennævnte oplysninger også angive de berørte kategorier af personoplysninger, kilden til personoplysningerne og, hvis det er relevant, om disse data stammer fra offentligt tilgængelige kilder. Disse oplysninger skal gives af den dataansvarlige inden for en rimelig frist efter indsamlingen af personoplysningerne, men senest inden for den første af følgende datoer i henhold til artikel 14, stk. 3, i GDPR: i) en måned under hensyn til de specifikke forhold, som personoplysningerne er behandlet under, ii) på tidspunktet for den første kommunikation med den registrerede, eller iii) hvis personoplysningerne er bestemt til videregivelse til en anden modtager, senest når personoplysningerne videregives første gang.

86. Der skal også gives nye oplysninger til registrerede, hvis videregives til en ny dataansvarlig. En vejhjælpstjeneste, der interagerer med opkoblede køretøjer, kan få oplysninger fra forskellige dataansvarlige afhængigt af det land eller den region, hvor der er behov for hjælp. Nye dataansvarlige bør give de registrerede de krævede oplysninger, når de registrerede

krydser grænser, og tjenester, der interagerer med opkoblede køretøjer, leveres af nye dataansvarlige.

87. Oplysningerne til de registrerede kan gives i lag[46], dvs. ved at adskille to informationsniveauer: først information på første niveau, som er de vigtigste for de registrerede, og derefter information, som vurderes at være af interesse på et senere tidspunkt. De vigtige oplysninger på første niveau omfatter ud over den dataansvarliges identitet, formålet med behandlingen og en beskrivelse af den registreredes rettigheder samt yderligere oplysninger om behandlingen, som har størst virkning på den registrerede, og behandling, der kan være overraskende for vedkommende. Databeskyttelsesrådet anbefaler, at den registrerede i forbindelse med opkoblede køretøjer gøres opmærksom på alle modtagere i det første informationslag. Som anført i WP29-retningslinjerne om gennemsigtighed bør dataansvarlige give oplysninger om de modtagere, der er mest relevante for registrerede. I praksis vil dette normalt være de navngivne modtagere, således at de registrerede ved præcis, hvem der har deres personoplysninger. Hvis dataansvarlige ikke oplyser navnene på modtagerne, bør oplysningerne være så specifikke som muligt med angivelse af typen af modtager (dvs. med henvisning til den virksomhed, den pågældende udfører), branche, sektor og delsektor og modtagernes placering.

88. De registrerede kan gives disse oplysninger gennem præcise og letforståelige bestemmelser i kontrakten om salget af køretøjet, i kontrakten om levering af tjenesteydelser og/eller et andet skriftligt middel, gennem særlige dokumenter (f.eks. køretøjsfabrikantens vedligeholdelsesdokumentation eller servicehåndbog) eller den køretøjsmonterede computer.

89. Der bør anvendes standardiserede ikoner ud over de krævede oplysninger, som fastsat i artikel 13 og 14 i GDPR, til at øge gennemsigtigheden ved potentielt at reducere behovet for at præsentere store mængder skriftlige oplysninger for den registrerede. Oplysningerne bør være synlige i køretøjet, så der med hensyn til den planlagte behandling gives et godt overblik, der er forståeligt og letlæseligt. Databeskyttelsesrådet understreger vigtigheden af at standardisere disse ikoner, så brugeren møder de samme symboler, uanset køretøjets mærke eller model. Når visse data, f.eks. positionen, indsamles, kan køretøjerne have et klart signal i køretøjet (f.eks. en lampe, der lyser i køretøjet) for at informere passagererne om, at der indsamles data.

## 2.6 Den registreredes rettigheder

90. Køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre dataansvarlige bør fremme de registreredes kontrol over deres data i hele behandlingsperioden ved at tilbyde dem specifikke værktøjer, som de kan bruge til effektivt at udøve deres rettigheder, navnlig deres ret til indsigt, berigtigelse og sletning, deres ret til at begrænse behandlingen og, afhængigt af retsgrundlaget for behandlingen, deres ret til dataportabilitet og til at gøre indsigelse.

91. For at gøre det lettere at ændre indstillingerne bør der indføres et profilstyringssystem, hvor præferencerne for kendte førere lagres, og som de til enhver tid kan bruge til nemt at ændre deres indstillinger for databeskyttelse. Profilstyringssystemet bør centralisere alle dataindstillinger for hver databehandling, især for at lette udøvelsen af retten til indsigt, sletning, fjernelse og portabilitet af personoplysninger fra køretøjssystemer efter den registreredes anmodning. Førerne bør kunne stoppe indsamlingen af visse typer data, midlertidig eller permanent, på ethvert tidspunkt, medmindre der er et specifikt retsgrundlag, som den dataansvarlige kan lægge til grund for sin fortsatte indsamling af specifikke data. Hvis der er tale om en kontrakt vedrørende et personligt tilpasset tilbud baseret på kørselsadfærd, finder denne kontrakt standardbetingelser da anvendelse på

[46] Se Artikel 29-Gruppen, Retningslinjer for gennemsigtighed i henhold til forordning 2016/679 (wp260rev.01), godkendt af Databeskyttelsesrådet.

brugeren. Disse funktioner bør aktiveres inden i køretøjet, selv om de også kan leveres til de registrerede gennem andre midler (f.eks. en særskilt applikation). For at sætte registrerede i stand til hurtigt og nemt at fjerne personoplysninger, som er lagret i bilens instrumentbræt (f.eks. GPS-navigationshistorik, webbrowsing osv.), anbefaler Databeskyttelsesrådet, at fabrikanterne stiller en simpel funktion til rådighed (f.eks. en sletknap).

92. Salget af et opkoblet køretøj og det deraf følgende skift af ejerskab bør også udløse en sletning af alle personoplysninger, der ikke længere er nødvendige til de tidligere nævnte formål, og den registrerede bør kunne udøve sin ret til portabilitet.

## 2.7 Sikkerhed

93. Køretøjs- og udstyrsfabrikanter, tjenesteudbydere og andre dataansvarlige bør indføre foranstaltninger, der garanterer sikkerheden og fortroligheden af behandlede data, og træffe alle nyttige foranstaltninger for at forhindre, at en uautoriseret person overtager kontrollen. Økonomiske aktører bør navnlig overveje at vedtage følgende foranstaltninger:

- kryptering af kommunikationskanalerne ved hjælp af en avanceret algoritme
- implementering af et system til administration af krypteringsnøgler, som er unikt for hvert køretøj, ikke kun for hver model
- kryptering af data, der lagres eksternt, ved hjælp af avancerede algoritmer
- regelmæssig fornyelse af krypteringsnøgler
- beskyttelse af krypteringsnøgler mod videregivelse
- autentifikation af datamodtagende enheder
- sikring af dataintegritet (f.eks. ved hjælp af hashing)
- krav om pålidelige brugerautentifikationsteknikker (adgangskode, elektronisk certifikat osv.) for at give adgang til personoplysninger.

94. Med hensyn til specifikt køretøjsfabrikanter anbefaler Databeskyttelsesrådet, at følgende sikkerhedsforanstaltninger gennemføres:

- adskillelse af køretøjets vitale funktioner fra de funktioner, der altid kræver en telekommunikationsforbindelse (f.eks. "infotainment")
- gennemførelse af tekniske foranstaltninger, der sætter køretøjsfabrikanterne i stand til hurtigt at imødegå sikkerhedsmæssige svagheder i køretøjets samlede levetid
- prioritering af sikre kommunikationsmidler, som specifikt anvendes til transport, til køretøjets vitale funktioner, så vidt muligt
- etablering af et alarmsystem, hvis køretøjets systemer angribes, med mulighed for drift ved nedsat funktionsniveau[47]
- lagring af en loghistorik over adgangen til køretøjets informationssystem, som f.eks. går op til seks måneder tilbage, for at gøre det muligt at fastslå kilden til et eventuelt angreb og regelmæssigt gennemgå de registrerede oplysninger for at opdage eventuelle usædvanlige forhold.

95. Disse generelle anbefalinger bør suppleres af specifikke krav under hensyntagen til hver databehandlings særlige forhold og formål.

[47] Nedsat funktionsniveau er et funktionsniveau for køretøjet, hvor de funktioner, der er nødvendige for dets sikre drift (dvs. minimumssikkerhedskrav), garanteres, selv om andre mindre vigtige funktioner deaktiveres (f.eks. anses navigationssystemet som ikkevæsentligt i modsætning til bremsesystemet).

## 2.8 Videregivelse af personoplysninger til tredjemand

96. I princippet har kun den dataansvarlige og den registrerede adgang til data, der genereres af et opkoblet køretøj. Den dataansvarlige kan imidlertid videregive personoplysninger til en kommerciel partner (modtager), for så vidt som denne overførsel er baseret på et af de retsgrundlag, der er anført i artikel 6 i GDPR.

97. I lyset af den mulige følsomhed af data om køretøjsbrugen (f.eks. data om ruter eller kørestil) anbefaler Databeskyttelsesrådet, at den registreredes samtykke systematisk skal indhentes, inden vedkommendes data overføres til en kommerciel partner, der handler som dataansvarlig (f.eks. ved at markere et felt, der ikke er markeret på forhånd, eller, hvis det er teknisk muligt, ved brug af en fysisk eller logisk enhed, som personen kan få adgang til fra køretøjet). Den kommercielle partner bliver da ansvarlig for de data, vedkommende modtager, og er omfattet af alle bestemmelserne i GDPR.

98. Køretøjsfabrikanten, tjenesteudbyderen eller en anden dataansvarlig kan overføre personoplysninger til en databehandler, der er udvalgt til at medvirke ved leveringen af tjenesten til den registrerede, såfremt databehandleren ikke anvender disse data til eget formål. Dataansvarlige og databehandlere skal udforme en kontrakt eller et andet juridisk dokument, som fastsætter hver parts forpligtelser og omfatter bestemmelserne i artikel 28 i GDPR.

## 2.9 Overførsel af data uden for EU/EØS

99. Når personoplysninger overføres til lande uden for Det Europæiske Økonomiske Område, er der fastlagt særlige garantier for at sikre, at beskyttelsen følger dataene.

100. Den dataansvarlige må følgelig kun overføre personoplysninger til en modtager, for så vidt som denne overførsel sker i overensstemmelse med kravene i kapitel V i GDPR.

## 2.10 Brug af køretøjsmonterede Wi-Fi-teknologier

101. Udviklingen inden for mobilteknologien har gjort det muligt nemt at anvende internettet på køreture. Det er muligt at etablere Wi-Fi-konnektivitet i et køretøj via et smartphone-hotspot eller en dedikeret enhed (OBD-II-dongle, trådløst modem eller router osv.), men de fleste fabrikanter tilbyder i dag modeller med indbygget mobildataforbindelse og modeller, som også kan oprette Wi-Fi-net. Afhængigt af situationen skal der tages hensyn til forskellige aspekter:

- Wi-Fi-konnektiviteten tilbydes som en tjeneste af en erhvervsdrivende, f.eks. en taxichauffør til sine kunder. I dette tilfælde kan den erhvervsdrivende eller vedkommendes virksomhed anses for en internettjenesteudbyder (ISP) og er dermed underlagt specifikke forpligtelser og begrænsninger med hensyn til behandlingen af kundernes personoplysninger.

- Wi-Fi-konnektiviteten er etableret alene til førerens brug (og udelukker dermed passagererne). I dette tilfælde anses behandlingen af personoplysninger for en rent personlig eller familiemæssig aktivitet i overensstemmelse med artikel 2, stk. 2, litra c), i GDPR og betragtning 18 til samme forordning.

102. Generelt indebærer udbredelsen af internetgrænseflader via Wi-Fi større risici for personers databeskyttelse. Gennem deres køretøjer foretager brugerne kontinuerlig transmission, og de kan derfor identificeres og spores. Med henblik på at undgå sporing bør køretøjs- og udstyrsfabrikanter derfor montere udstyr, der nemt kan fravælges, og som sikrer, at SSID'en (service set identifier) for det køretøjsmonterede Wi-Fi-net ikke indsamles.

# 3 CASESTUDIER

103. I dette afsnit beskrives fem specifikke eksempler på behandling i forbindelse med opkoblede køretøjer, som svarer til de scenarier, som interessenter i sektoren sandsynligvis vil støde på. Eksemplerne dækker databehandling, som kræver beregningskapacitet, der ikke kan mobiliseres lokalt i køretøjet, og/eller overførsel af personoplysninger til tredjemand med henblik på yderligere analyse og eller tilvejebringelse af yderligere funktionalitet eksternt. For hver type behandling angives de tiltænkte formål, kategorierne af indsamlede data, opbevaringsperioden for sådanne data, de registreredes rettigheder, de sikkerhedsforanstaltninger, der skal gennemføres, og modtagerne af oplysningerne i dette dokument. Hvis nogle af disse områder ikke er beskrevet i det følgende, finder de generelle anbefalinger i den foregående del anvendelse.

104. De valgte eksempler er ikke-udtømmende og er alene vejledende med hensyn til de mange forskellige typer behandling, retsgrundlag, aktører osv., der kan forekomme i forbindelse med opkoblede køretøjer.

## 3.1 Levering af en tjeneste ved en tredjemand

105. Registrerede kan indgå kontrakt med en tjenesteudbyder for at få adgang til værdiforøgende tjenester i forbindelse med deres køretøj. En registreret kan f.eks. tegne en brugsbaseret forsikringspolice, som tilbyder lavere forsikringspræmier for mindre kørsel ("Pay As You Drive") eller god kørselsadfærd ("Pay How You Drive"), og som gør det nødvendigt, at forsikringsselskabet overvåge vedkommendes kørselsvaner. En registreret kan også indgå kontrakt med en virksomhed, der tilbyder vejhjælp i tilfælde af f.eks. motorstop, og som indebærer, at køretøjets position overføres til virksomheden eller en tjenesteudbyder, så de modtager meddelelser eller advarsler om køretøjets funktion (f.eks. en advarsel om slidte bremser eller en påmindelse om datoen for teknisk inspektion).

### 3.1.1 Brugsbaseret forsikring

106. "Pay as you drive" er en type brugsbaseret forsikring, som sporer førerens kilometertal og/eller kørselsvaner med henblik på at udskille og belønne "sikre" førere gennem lavere præmier. Forsikringsselskabet kræver, at føreren monterer en indbygget telematiktjeneste, anvender en mobilapplikation eller aktiverer et fabriksindbygget modul, der sporer policeindehaverens kilometertal og/eller kørselsadfærd (bremsemønster, hurtig acceleration osv.). De oplysninger, der indsamles af telematikenheden, bruges til at tildele føreren scorer og analysere, hvilke risici vedkommende udgør for forsikringsselskabet.

107. En brugsbaseret forsikring kræver samtykke i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, og Databeskyttelsesrådet finder derfor, at policeindehaveren skal have mulighed for at tegne en forsikringspolice, der ikke er brugsbaseret. Ellers anses samtykke ikke for at være givet frit, da opfyldelsen af kontrakten ellers ville være betinget af samtykke. I henhold til artikel 7, stk. 3, i GDPR skal en registreret desuden have mulighed for at trække sit samtykke tilbage.

#### *3.1.1.1 Retsgrundlag*

108. Når data indsamles gennem en offentligt tilgængelig elektronisk kommunikationstjeneste (f.eks. via SIM-kortet i telematikenheden), kræves der samtykke for at få adgang til oplysninger, der allerede er lagret i køretøjet som fastsat i e-databeskyttelsesdirektivets artikel 5, stk. 3. Ingen af de undtagelser, der er anført i disse bestemmelser, finder anvendelse i denne sammenhæng: Behandlingen foretages ikke alene med det formål at overføre kommunikation via et elektronisk kommunikationsnet, og den vedrører heller ikke en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkeligt har anmodet om. Samtykke bør indhentes ved kontraktens indgåelse.

109. Med hensyn til behandlingen af personoplysninger efter lagringen eller adgangen til slutbrugerens terminaludstyr kan forsikringsselskabet henholde sig til artikel 6, stk. 1, litra b), i GDPR i denne specifikke sammenhæng, såfremt det kan fastslås, at behandlingen foretages i overensstemmelse med en gyldig kontrakt med den registrerede, og at behandlingen er nødvendig for, at den pågældende kontrakt med den registrerede kan opfyldes. For så vidt som behandlingen er objektivt nødvendig for opfyldelsen af kontrakten med den registrerede, finder Databeskyttelsesrådet, at anvendelsen af artikel 6, stk. 1, litra b), i GDPR ikke vil reducere den yderligere beskyttelse, der opnås med e-databeskyttelsesdirektivets artikel 5, stk. 3, i dette specifikke eksempel. Dette retsgrundlag materialiseres af den registrerede, når denne underskriver en kontrakt med forsikringsselskabet.

#### *3.1.1.2 Indsamlede data*

110. To typer personoplysninger skal tages i betragtning:

- **kommercielle data og transaktionsdata:** den registreredes identifikationsdata, transaktionsdata, data vedrørende betalingsmidler osv.

- **brugsdata**: personoplysninger, der genereres af køretøjet, kørselsvaner, position osv.

111. Databeskyttelsesrådet anbefaler — for så vidt muligt og i lyset af risikoen for, at data, der indsamles via telematikenheden, kan misbruges til at oprette en præcis profil af førerens bevægelser — at data vedrørende kørselsadfærd behandles:

- i køretøjet i telematikenheder eller i brugerens smartphone, således at forsikringsselskabet kun har adgang til resultatdataene (f.eks. en score vedrørende kørselsvaner), ikke til de detaljerede rådata (se afsnit 2.1)

- eller af telematikudbyderen på vegne af den dataansvarlige (forsikringsselskabet) med henblik på at generere numeriske scorer, der overføres til forsikringsselskabet med faste mellemrum. I dette tilfælde skal rådata og data, der direkte vedrører førerens identitet, holdes adskilte.

Det betyder, at telematikudbyderen modtager realtidsdata, men ikke kender policeindehavernes navne, registreringsnumre osv. Forsikringsselskabet kender på den anden side policeindehavernes navne, men modtager kun scorerne og de samlede kilometertal, ikke de rådata, der blev anvendt til at generere disse scorer.

112. Det skal desuden bemærkes, at lokaliseringsdata ikke må indsamles, hvis kun kilometerantallet er nødvendigt for at opfylde kontrakten.

#### *3.1.1.3 Opbevaringsperiode*

113. I forbindelse med databehandling, der foretages med henblik på at opfylde en kontrakt (dvs. levering af en tjeneste), skal der skelnes mellem to typer data, inden deres respektive opbevaringsperioder fastlægges:

- **Kommercielle data og transaktionsdata:** Disse data kan opbevares i en aktiv database i hele kontraktens løbetid. Ved kontraktens udløb kan de arkiveres fysisk (på et særskilt medie: DVD osv.) eller logisk (ved autorisationsstyring) i tilfælde af en eventuel tvist. Efter udløbet af de lovbestemte forældelsesfrister slettes eller anonymiseres dataene.

- **Brugsdata:** Brugsdata kan klassificeres som rådata og aggregerede data. Som anført ovenfor bør dataansvarlige og databehandlere så vidt muligt ikke behandle rådata. Hvis det er nødvendigt, bør rådata kun opbevares, så længe de er nødvendige for at uddybe de aggregerede data og til at kontrollere gyldigheden af den pågældende aggregeringsproces. Aggregerede data bør kun opbevares, så længe det er nødvendigt for at levere tjenesten, eller som det ellers kræves i henhold til EU-retten eller en medlemsstats nationale ret

#### *3.1.1.4 Registreredes oplysning og rettigheder*

114. Inden behandlingen af personoplysninger skal den registrerede oplyses herom i henhold til artikel 13 i GDPR på en gennemsigtig og forståelig måde. Den registrerede skal navnlig oplyses om det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum. I sidstnævnte tilfælde anbefaler Databeskyttelsesrådet, at der benyttes en pædagogisk metode til at understrege forskellen mellem rådata og den score, der genereres på dette grundlag, idet det understreges, at forsikringsselskabet i dette tilfælde kun indsamler resultatet af scoren, når det er hensigtsmæssigt.

115. Hvis data ikke behandles i køretøjet, men af en telematikudbyder på vegne af den dataansvarlige (forsikringsselskabet), kan det i denne forbindelse nævnes, at udbyderen ikke har adgang til data, der direkte vedrører førerens identitet (f.eks. navn, registreringsnummer osv.). I lyset af vigtigheden af, at registrerede oplyses om konsekvenserne af behandlingen af deres personoplysninger, og den omstændighed, at registrerede ikke bør blive overrasket over behandlingen af deres personoplysninger, anbefaler Databeskyttelsesrådet, at den registrerede oplyses om eksistensen af profilering og konsekvenserne af sådan profilering, selv om den ikke indebærer automatiske afgørelser som omhandlet i artikel 22 i GDPR.

116. Med hensyn til de registreredes rettigheder skal de udtrykkeligt oplyses om de midler, de kan benytte til at udøve deres rettigheder til indsigt, berigtigelse, begrænsning og sletning. Da rådata, der indsamles i denne sammenhæng, leveres af den registrerede (gennem specifikke formularer eller gennem vedkommendes aktivitet) og behandles på grundlag af artikel 6, stk. 1, litra b), i GDPR (opfyldelse af en kontrakt), har den registrerede ret til at udøve sin ret til dataportabilitet. Som det fremhæves i retningslinjerne om dataportabilitet, anbefaler Databeskyttelsesrådet på det kraftigste, "at dataansvarlige tydeligt forklarer

forskellen mellem de typer oplysninger, som en registreret kan modtage via registreredes rettighederne til indsigt og dataportabilitet"[48].

117. Oplysningerne kan gives, når kontrakten er underskrevet.

#### *3.1.1.5 Modtager:*

118. Databeskyttelsesrådet anbefaler, at køretøjets brugsdata så vidt muligt behandles direkte i telematikenheder, så forsikringsselskabet kun har adgang til resultatdata (f.eks. en score), ikke til de detaljerede rådata.

119. Hvis en telematikudbyder indsamler dataene på vegne af den dataansvarlige (forsikringsselskabet) med henblik på at generere numeriske scorer, behøver den ikke kende førerens identitet (f.eks. navn, registreringsnummer osv.) for policeindehaverne.

#### *3.1.1.6 Sikkerhed:*

120. De generelle anbefalinger finder anvendelse. Se afsnit 2.7.

### 3.1.2 Leje og reservation af parkeringsplads

121. Ejeren af en parkeringsplads ønsker at udleje den. Til det formål indsætter ejeren et opslag med pladsen og en pris i en webapplikation. Når parkeringspladsen vises, sender applikationen ejeren en meddelelse, når en fører ønsker at reservere den. Føreren kan vælge en destination og tjekke, om der er ledige parkeringspladser ud fra forskellige kriterier. Efter ejerens godkendelse bekræftes transaktionen, og tjenesteudbyderen håndterer betalingstransaktionen og bruger derefter navigation til at køre til stedet.

#### *3.1.2.1 Retsgrundlag*

122. Når data indsamles via et offentligt tilgængeligt elektronisk kommunikationsnet, finder e-databeskyttelsesdirektivets artikel 5, stk. 3, anvendelse.

123. Dette er en informationssamfundstjeneste, og der kræves derfor i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, ikke samtykke for at få adgang til oplysninger, som allerede er lagret i køretøjet, når abonnenten udtrykkeligt anmoder om en sådan tjeneste.

124. For behandlingen af personoplysninger og kun de data, der er nødvendige for at opfylde den kontrakt, som den registrerede har indgået, er artikel 6, stk. 1, litra b), i GDPR retsgrundlaget.

#### *3.1.2.2 Indsamlede data*

125. De behandlede data omfatter førerens kontaktoplysninger (navn, e-mail. telefonnummer, køretøjstype (f.eks. bil, lastbil eller motorcykel), registreringsnummer, parkeringstid, betalingsoplysninger (f.eks. kreditkortoplysninger) og navigationsdata.

#### *3.1.2.3 Opbevaringsperiode*

126. Data bør kun opbevares, så længe de er nødvendige for at opfylde parkeringskontrakten, eller som det ellers kræves i henhold til EU-retten eller en medlemsstats nationale ret. Derefter anonymiseres eller slettes dataene.

#### *3.1.2.4 Registreredes oplysning og rettigheder*

127. Inden behandlingen af personoplysninger skal den registrerede oplyses herom i henhold til artikel 13 i GDPR på en gennemsigtig og forståelig måde.

128. Den registrerede skal udtrykkeligt oplyses om de midler, vedkommende kan benytte til at udøve sine rettigheder til indsigt, berigtigelse, begrænsning og sletning. Da data, der indsamles i denne sammenhæng, leveres af den registrerede (gennem specifikke formularer eller gennem vedkommendes aktivitet) og behandles på grundlag af artikel 6, stk. 1, litra b),

[48] Artikel 29-Gruppen, Retningslinjer vedrørende retten til dataportabilitet i henhold til forordning (EU) 2016/676, WP242 rev.01, godkendt af Databeskyttelsesrådet, s. 13.

i GDPR (opfyldelse af en kontrakt), har den registrerede ret til at udøve sin ret til dataportabilitet. Som det fremhæves i retningslinjerne om dataportabilitet, anbefaler Databeskyttelsesrådet på det kraftigste, "at dataansvarlige tydeligt forklarer forskellen mellem de typer oplysninger, som en registreret kan modtage via registreredes rettighederne til indsigt og dataportabilitet".

#### *3.1.2.5 Modtager:*

129. I princippet har kun den dataansvarlige og databehandleren adgang til dataene.

#### *3.1.2.6 Sikkerhed:*

130. De generelle anbefalinger finder anvendelse. Se afsnit 2.7.

## 3.2 eCall

131. I tilfælde af en alvorlig ulykke i EU udløser køretøjet automatisk et elektronisk opkald til 112, det EU-dækkende alarmnummer (se afsnit 1.1 for yderligere detaljer), som gør det muligt straks at sende en ambulance til ulykkesstedet i overensstemmelse med forordning (EU) 2015/758 af 29. april 2015 om typegodkendelseskrav for indførelse af et køretøjsmonteret eCall-system, der er baseret på 112-tjenesten, og om ændring af direktiv 2007/46/EF ("forordning (EU) 2015/758").

132. Den eCall-generator, der er installeret i køretøjet, som muliggør transmission via et offentligt mobilt trådløst kommunikationsnet, initierer et nødopkald, som udløses automatisk af køretøjets sensorer eller manuelt af personerne i køretøjet i tilfælde af en ulykke. Ud over aktiveringen af lydkanalen omfatter den anden hændelse, der automatisk udløses som følge af en ulykke, generering af et MSD (Minimum Set of Data), som sendes til den nærmeste alarmcentral (Public Safety Answering Point, PSAP).

### 3.2.1 Retsgrundlag

133. Med hensyn til anvendelsen af e-databeskyttelsesdirektivet skal to bestemmelser tages i betragtning:

- artikel 9 vedrørende lokaliseringsdata, bortset fra trafikdata, som kun finder anvendelse på elektroniske kommunikationstjenester

- artikel 5, stk. 3, vedrørende adgang til oplysninger, der er lagret på den generator, der er monteret i køretøjet.

134. Selv om disse bestemmelser i princippet kræver den registreredes samtykke, udgør forordning (EU) 2015/758 en retlig forpligtelse, som den dataansvarlige er underlagt (den registrerede har ikke et reelt eller frit valg og kan ikke afvise behandlingen af sine data). Forordning (EU) 2015/758 tilsidesætter derfor kravet om førerens samtykke til behandlingen af lokaliseringsdata og MSD[49].

135. Retsgrundlaget for behandlingen af disse data vil være overholdelsen af en retlig forpligtelse som fastsat i artikel 6, stk. 1, litra c), i GDPR (dvs. forordning (EU) 2015/758).

### 3.2.2 Indsamlede data

136. I henhold til forordning (EU) 2015/578 indeholder de data, som udsendes af det 112-baserede køretøjsmonterede eCall-system kun de minimumsoplysninger, der er omhandlet i standarden EN 15722: 2015 "Intelligente transportsystemer — eSafety — eCall-minimumsdatasæt", herunder:

[49] Det skal bemærkes, at artikel 8, stk. 1, litra f), i Rådets mandat til forhandling om forslaget til en forordning om e-databeskyttelse ikke omhandler en specifik undtagelse for eCall, da samtykke ikke kræves, når *"det er nødvendigt at lokalisere terminaludstyr, når en slutbruger foretager et nødopkald enten til det EU-dækkende alarmnummer "112" eller et nationalt alarmnummer, i henhold til artikel 13, stk. 3)".*

- angivelse af, om eCall er blevet udløst manuelt eller automatisk
- køretøjets type
- køretøjets identifikationsnummer (VIN)
- typen af køretøjets fremdriftssystem
- tidsstemplet for genereringen af den indledende meddelelse for den aktuelle eCall-hændelse
- køretøjets sidst kendte geografiske position (breddegrad og længdegrad) bestemt så tæt på genereringen af meddelelsen som muligt
- køretøjets sidst kendte faktiske kørselsretning bestemt så tæt på genereringen af meddelelsen som muligt (kun køretøjets tre sidste positioner).

### 3.2.3 Opbevaringsperiode

137. I henhold til forordning (EU) 2015/758 må data ikke lagres i længere tid end nødvendigt med henblik på at håndtere nødsituationer. Disse oplysninger slettes helt, så snart de ikke længere er nødvendige til dette formål. Data i eCall-systemets interne hukommelse fjernes desuden automatisk og løbende. Det er kun tilladt at lagre køretøjets tre sidste positioner, for så vidt det er strengt nødvendigt med henblik på at bestemme den nuværende position og kørselsretningen på tidspunktet for begivenheden.

### 3.2.4 Registreredes oplysning og rettigheder

138. I henhold til artikel 6 i forordning (EU) 2015/758 skal fabrikanterne give klare og udførlige oplysninger om databehandling, der foretages ved brug af eCall-systemet. Disse oplysninger skal gives særskilt i ejerens instruktionsbog for det 112-baserede køretøjsmonterede eCall-system og for eCall-systemet understøttet af tredjepartstjenester, inden det pågældende system tages i brug. Det omfatter:

- henvisning til retsgrundlaget for databehandlingen
- den omstændighed, at det 112-baserede køretøjsmonterede eCall-system er aktiveret som standardindstilling
- ordningerne for den databehandling, som det 112-baserede køretøjsmonterede eCall-system foretager
- eCall-databehandlingens specifikke formål, som begrænses til de nødsituationer, der er omhandlet i artikel 5, stk. 2, første afsnit, i forordning (EU) 2015/758
- de typer data, der indsamles og behandles, og dem, der modtager disse data
- tidsgrænsen for lagring af data i det 112-baserede køretøjsmonterede eCall-system
- den omstændighed, at der ikke er konstant sporing af køretøjet
- ordningerne for udøvelsen af den registreredes rettigheder og den kontakttjeneste, der er kompetent til at behandle anmodninger om adgang
- eventuelle nødvendige yderligere oplysninger om sporbarhed, sporing og behandling af personoplysninger i forbindelse med levering af en eCall-tjeneste understøttet af tredjepartstjenester og/eller andre tillægstjenester, hvilket forudsætter, at ejeren udtrykkeligt har givet sit samtykke, og at GDPR er overholdt. Der skal tages særligt hensyn til, at der kan være forskelle mellem den databehandling, der udføres gennem det 112-baserede køretøjsmonterede eCall-system, og den databehandling, der udføres gennem eCall-systemer understøttet af tredjepartstjenester eller andre tillægstjenester.

139. Tjenesteudbyderen skal endvidere også give de registrerede oplysninger i overensstemmelse med artikel 13 i GDPR på en gennemsigtig og forståelig måde. Den registrerede skal navnlig oplyses om formålene med behandlingen af personoplysninger og det forhold, at behandlingen af personoplysninger er baseret på en retlig forpligtelse, som den dataansvarlige er underlagt.

140. Under hensyntagen til behandlingens karakter skal oplysningerne om modtagerne eller kategorierne af modtagere af personoplysningerne være tydelige, og de registrerede skal oplyses om, at dataene ikke må være tilgængelige for enheder uden for det 112-baserede køretøjsmonterede eCall-system, inden et eCall udløses.

141. Med hensyn til registreredes rettigheder skal det bemærkes, at retten til indsigelse og retten til portabilitet ikke finder anvendelse, da behandlingen er baseret på en retlig forpligtelse.

#### 3.2.5 Modtager:

142. Disse data må ikke være tilgængelige for enheder uden for det 112-baserede køretøjsmonterede eCall-system, inden et eCall udløses.

143. Når det udløses (enten manuelt af personerne i køretøjet eller automatisk, når en køretøjsmonteret sensor registrerer et alvorligt sammenstød), etablerer eCall-systemet en lydforbindelse til den relevante alarmcentral, og minimumsdatasættet sendes til alarmcentraloperatøren.

144. Data, der overføres via det 112-baserede køretøjsmonterede eCall-system, og som behandles af alarmcentralerne, kan desuden kun overføres til de beredskabstjenester og tjenestepartnere, der er omhandlet i afgørelse nr. 585/2014/EU, i tilfælde af hændelser med relation til eCalls og på de betingelser, der er fastsat i nævnte afgørelse, samt når de udelukkende anvendes til at opfylde formålene med den nævnte afgørelse. Data, der behandles af alarmcentralerne via det 112-baserede køretøjsmonterede eCall-system, overføres ikke til andre tredjeparter uden udtrykkeligt samtykke fra den registrerede.

#### 3.2.6 Sikkerhed

145. Forordning (EU) 2015/758 fastsætter kravene om, at der i eCall-systemet skal indbygges teknologier, der styrker beskyttelsen af privatlivets fred, med henblik på at sikre brugerne det fornødne niveau af beskyttelse af privatlivets frem, og de garantier, der er nødvendige for at forebygge overvågning og misbrug. Fabrikanterne skal desuden sikre, at det 112-baserede eCall-system og andre systemer, der foretager et eCall, der håndteres af tredjepartstjenester eller andre tillægstjenester, er udformet, så det ikke kan udveksles personoplysninger mellem disse systemer.

146. Med hensyn til alarmcentraler bør medlemsstaterne sikre, at personoplysninger beskyttes mod misbrug, herunder ulovlig adgang, ændring eller tab, og at der indføres bestemmelser for opbevaring af personoplysninger, opbevaringens varighed, behandling og beskyttelse på det hensigtsmæssige niveau, og at disse bestemmelser overholdes til fulde.

### 3.3 Ulykkesundersøgelser

147. Registrerede kan frivilligt acceptere at deltage i ulykkesundersøgelser, som har til formål at fremskaffe mere viden om årsagerne til trafikulykker og mere generelt til videnskabelige formål.

#### 3.3.1 Retsgrundlag

148. Når data indsamles via en offentlig elektronisk kommunikationstjeneste, skal den dataansvarlige indhente den registreredes samtykke for at få adgang til oplysninger, som allerede er lagret i køretøjet, som fastsat i e-databeskyttelsesdirektivets artikel 5, stk. 3. Ingen af de undtagelser, der er anført i disse bestemmelser, finder anvendelse i denne sammenhæng: Behandlingen foretages ikke alene med det formål at overføre

kommunikation via et elektronisk kommunikationsnet, og den vedrører heller ikke en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkeligt har anmodet om.

149. Med hensyn til behandlingen af personoplysninger og under hensyntagen til varieteten og mængden af personoplysninger, der kræves til ulykkesundersøgelser, anbefaler Databeskyttelsesrådet, at behandlingen baseres på den registreredes forudgående samtykke i henhold til artikel 6 i GDPR. Et sådant forudgående samtykke skal gives på en specifik formular, hvorigennem den registrerede frivilligt accepterer at deltage i undersøgelsen og få sine personoplysninger behandlet til dette formål. Samtykket skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den person, hvis data behandles (f.eks. ved at markere et felt, der ikke er markeret på forhånd, eller ved at konfigurere den køretøjsmonterede computer til at aktivere en funktion i køretøjet). Et sådant samtykke skal gives særskilt til forskellige formål, må ikke være sammenknyttet med kontrakten om køb eller leasing af en ny bil, og det skal være lige så nemt at tilbagetrække samtykket som at give det. Ved tilbagetrækning af samtykke skal behandlingen stoppes. Dataene skal derfor slettes fra den aktive database eller anonymiseres.

150. Samtykke som krævet i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, og samtykke, der kræves som retsgrundlag for behandlingen af data kan indhentes samtidig (f.eks. ved at markere et felt, der tydeligt angiver, hvad den registrerede giver samtykke til).

151. Det skal bemærkes, at der — afhængigt af betingelserne for behandlingen (den dataansvarlige art osv.) — lovligt kan vælges et andet retsgrundlag, så længe det ikke reducere den yderligere beskyttelse, der er fastsat ved e-databeskyttelsesdirektivets artikel 5, stk. 3 (se punkt 15). Hvis behandlingen er baseret på et andet retsgrundlag, f.eks. udførelsen af en opgave, som udføres i samfundets interesse (artikel 6, stk. 1, litra e), i GDPR), anbefaler Databeskyttelsesrådet, at de registrerede medtages i undersøgelsen på et frivilligt grundlag.

### 3.3.2 Indsamlede data

152. Den dataansvarlige må indsamle personoplysninger, der er strengt nødvendige for behandlingen.

153. To typer data skal tages i betragtning:

- **data vedrørende deltagere og køretøjer**
- **tekniske data fra køretøjer** (øjeblikkelig hastighed osv.).

154. Videnskabelig forskning i forbindelse med ulykkesundersøgelser begrunder indsamlingen af den øjeblikkelige hastighed, herunder af juridiske personer, der ikke i streng forstand udfører en opgave i samfundets interesse.

155. Databeskyttelsesrådet finder, som anført ovenfor, at øjeblikkelig hastighed, der indsamles i forbindelse med ulykkesundersøgelser, ikke er overtrædelsesrelaterede data (dvs. at de ikke indsamles med henblik på at efterforske eller retsforfølge en lovovertrædelse), hvilket begrunder, at de indsamles af juridiske personer, der ikke i streng forstand udfører en opgave i samfundets interesse.

### 3.3.3 Opbevaringsperiode

156. Der skal skelnes mellem to typer data. For det første kan data vedrørende deltagere og køretøjer opbevares, så længe undersøgelsen varer. For det andet bør tekniske data fra køretøjerne opbevares så kort tid som muligt til formålet. I denne henseende forekommer fem år fra slutdatoen for undersøgelsen af være en rimelig periode. Efter udløbet af denne periode slettes eller anonymiseres dataene.

### 3.3.4 Registreredes oplysning og rettigheder

157. Inden behandlingen af personoplysninger skal den registrerede oplyses herom i henhold til artikel 13 i GDPR på en gennemsigtig og forståelig måde. Ved indsamling af den øjeblikkelige hastighed bør de registrerede specifikt informeres om dataindsamlingen. Da databehandlingen er baseret på samtykke, skal den registrerede specifikt oplyses om retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf. Da data, der indsamles i denne sammenhæng, leveres af den registrerede (gennem specifikke formularer eller gennem vedkommendes aktivitet) og behandles på grundlag af artikel 6, stk. 1, litra a), i GDPR (samtykke), har den registrerede ret til at udøve sin ret til dataportabilitet. Som det fremhæves i retningslinjerne om dataportabilitet, anbefaler Databeskyttelsesrådet på det kraftigste, "at dataansvarlige tydeligt forklarer forskellen mellem de typer oplysninger, som en registreret kan modtage via registreredes rettighederne til indsigt og dataportabilitet". Den dataansvarlige bør følgelig give den registrerede en nem mulighed for at trække sit samtykke tilbage, frit og når som helst, og bør udvikle værktøjer til at besvare anmodninger om dataportabilitet.

158. Disse oplysninger kan gives i forbindelse med underskrivelsen af formularen om deltagelse i ulykkesundersøgelsen.

### 3.3.5 Modtager

159. I princippet har kun den dataansvarlige og databehandleren adgang til dataene.

### 3.3.6 Sikkerhed

160. De indførte sikkerhedsforanstaltninger skal som nævnt være tilpasset dataenes følsomhedsniveau. Hvis øjeblikkelig hastighed (eller andre data vedrørende straffedomme og lovovertrædelser) indsamles som led i ulykkesundersøgelsen, anbefaler Databeskyttelsesrådet på det kraftigste, at der indføres effektive sikkerhedsforanstaltninger, herunder:

- gennemførelse af pseudonymiseringsforanstaltninger (f.eks. hashing af data såsom den registreredes efternavn/fornavn og serienummeret med en hemmelig nøgle)
- lagring af data vedrørende øjeblikkelig hastighed og position i særskilte databaser (f.eks. ved brug af en avanceret krypteringsmekanisme med særskilte nøgler og godkendelsesmekanismer)
- og/eller sletning af lokaliseringsdata, straks referencehændelsen eller sekvensen er kategoriseret (f.eks. vejtype, dag/nat), og lagring af direkte identificerbare data i en særskilt database, som kun få personer har adgang til.

## 3.4 Håndtering af biltyveri

161. Registrerede, hvis bil bliver stjålet, ønsker måske at forsøge at finde deres bil ved hjælp af lokalisering. Brugen af lokaliseringsdata er strengt begrænset til efterforskningen og de kompetente retlige myndigheders behandling af sagen.

### 3.4.1 Retsgrundlag

162. Når data indsamles via et offentligt tilgængeligt elektronisk kommunikationsnet, finder e-databeskyttelsesdirektivets artikel 5, stk. 3, anvendelse.

163. Dette er en informationssamfundstjeneste, og der kræves derfor i henhold til e-databeskyttelsesdirektivets artikel 5, stk. 3, ikke samtykke for at få adgang til oplysninger, som allerede er lagret i køretøjet, når abonnenten udtrykkeligt anmoder om en sådan tjeneste.

164. Med hensyn til behandlingen af personoplysninger er retsgrundlaget for behandlingen af lokaliseringsdata køretøjsejerens samtykke eller opfyldelsen af en kontrakt (kun for de data, der er nødvendige for at opfylde den kontrakt, som køretøjets ejer har indgået).

165. Samtykket skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den person, hvis data behandles (f.eks. ved at markere et felt, der ikke er markeret på forhånd, eller ved at konfigurere den køretøjsmonterede computer til at aktivere en funktion i køretøjet). Frihed til at give samtykke indebærer muligheden for til enhver tid at trække samtykket tilbage, som den registrerede udtrykkeligt skal informeres om. Ved tilbagetrækning af samtykke skal behandlingen stoppes. Dataene skal da slettes fra den aktive database, anonymiseres eller arkiveres.

### 3.4.2 Indsamlede data

166. Lokaliseringsdata må kun overføres ved anmeldelsen af tyveriet og må ikke indsamles løbende resten af tiden.

### 3.4.3 Opbevaringsperiode

167. Lokaliseringsdata må kun opbevares i det tidsrum, hvor sagen behandles af de kompetente retlige myndigheder, eller indtil afslutningen af en afklarende procedure, som ikke ender med, at tyveriet af køretøjet bekræftes.

### 3.4.4 Information af de registrerede

168. Inden behandlingen af personoplysninger skal den registrerede oplyses herom i henhold til artikel 13 i GDPR på en gennemsigtig og forståelig måde. Databeskyttelsesrådet anbefaler mere specifikt, at den dataansvarlige understreger, at der ikke foretages konstant sporing af køretøjet, og at lokaliseringsdata kun må indsamles og overføres ved tyverianmeldelsen. Den dataansvarlige skal desuden give den registrerede oplysninger om det forhold, at kun godkendte medarbejdere på den eksterne overvågningsplatform og godkendte myndigheder har adgang til dataene.

169. For så vidt angår de registreredes rettigheder, skal den registrerede — da databehandlingen er baseret på samtykke — specifikt oplyses om retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf. Når de data, der indsamles i denne sammenhæng, leveres af den registrerede (gennem specifikke formularer eller gennem vedkommendes aktivitet) og behandles på grundlag af artikel 6, stk. 1, litra a) (samtykke) eller litra b) (opfyldelse af en kontrakt) i GDPR, har den registrerede ret til at udøve sin ret til dataportabilitet. Som det fremhæves i retningslinjerne om dataportabilitet, anbefaler Databeskyttelsesrådet på det kraftigste, "at dataansvarlige tydeligt forklarer forskellen mellem de typer oplysninger, som en registreret kan modtage via registreredes rettighederne til indsigt og dataportabilitet".

170. Den dataansvarlige bør følgelig give den registrerede en nem mulighed for at trække sit samtykke tilbage (når samtykke udgør retsgrundlaget), frit og når som helst, og bør udvikle værktøjer til at besvare anmodninger om dataportabilitet.

171. Oplysningerne kan gives, når kontrakten er underskrevet.

### 3.4.5 Modtagere

172. I tilfælde af en tyverianmeldelse kan lokaliseringsdata videregives til i) godkendte medarbejdere på den eksterne overvågningsplatform og ii) godkendte myndigheder.

### 3.4.6 Sikkerhed

173. De generelle anbefalinger finder anvendelse. Se afsnit 2.7.