Riktlinjer 01/2020 om behandling av personuppgifter i samband med uppkopplade fordon och rörlighetsrelaterade applikationer

Version 2.0

Antagna den 9 mars 2021

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

Versionshistorik

Version 2.0	9 mars 2021	Antagande av riktlinjerna efter offentligt samråd
Version 1.0	28 januari 2020	Antagande av riktlinjerna inför offentligt samråd

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande riktlinjer

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING

1. Bilen är en symbol för 1900-talets ekonomi och en av de masskonsumtionsprodukter som har påverkat samhället som helhet. Bilar förknippas i allmänhet med frihet och betraktas ofta som mer än bara ett transportmedel. De representerar ett privat område där människor kan åtnjuta en form av självständigt beslutsfattande, utan att stöta på någon yttre inblandning. I dag blir uppkopplade fordon allt vanligare och en sådan vision motsvarar därför inte längre verkligheten. Konnektivitet i fordon sprider sig i snabb takt från lyxmodeller och premiummärken till modeller i mellansegmentet med hög försäljningsvolym, och fordon håller på att bli enorma datanav. Inte bara fordon, utan även förare och passagerare blir allt mer uppkopplade. Många modeller som lanserats på marknaden under de senaste åren integrerar i själva verket sensorer och ansluten fordonsburen utrustning, som bland annat kan samla in och registrera motorprestanda, körvanor, besökta platser och eventuellt även förarens ögonrörelser, puls eller biometriska uppgifter i syfte att unikt identifiera en fysisk person[2].

2. Sådan behandling av uppgifter sker i ett komplext ekosystem, som inte är begränsat till de traditionella aktörerna i bilindustrin utan också formas av tillkomsten av nya aktörer som hör till den digitala ekonomin. Dessa nya aktörer kan erbjuda infotainmenttjänster såsom onlinemusik, information om vägförhållanden och trafik eller tillhandahålla system och tjänster för förarassistans, såsom autopilot, uppdateringar om fordonets skick, användningsbaserad försäkring eller dynamiska kartor. Eftersom fordon är uppkopplade via elektroniska kommunikationsnät spelar även de väghållare och teleoperatörer som är involverade i denna process en viktig roll när det gäller den eventuella behandlingen av förarnas och passagerarnas personuppgifter.

3. Dessutom genererar uppkopplade fordon allt fler uppgifter, varav de flesta kan betraktas som personuppgifter eftersom de avser förare eller passagerare. Även om de uppgifter som samlas in av en uppkopplad bil inte är direkt kopplade till ett namn utan till fordonets tekniska aspekter och egenskaper kommer de att angå bilens förare eller passagerare. Som

[1] Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.
[2] Infografik, *Data and the connected car* från Future of Privacy Forum, https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

exempel kan uppgifter om körstil eller tillryggalagd sträcka, uppgifter om slitage på fordonsdelar, lokaliseringsuppgifter eller uppgifter som samlas in av kameror avse förarens beteende samt information om andra personer som kan befinna sig i fordonet eller registrerade som passerar förbi. Sådana tekniska uppgifter produceras av en fysisk person och gör det möjligt för den personuppgiftsansvarige eller en annan person att direkt eller indirekt identifiera honom eller henne. Fordonet kan betraktas som en terminal som kan användas av olika användare. Liksom för en persondator påverkar därför denna potentiella mångfald av användare inte uppgifternas personliga karaktär.

4. År 2016 genomförde *Fédération Internationale de l'Automobile* (FIA) en kampanj i Europa kallad ”My Car My Data” för att få en uppfattning om vad européerna tycker om uppkopplade bilar[3]. Även om den visade på ett stort intresse hos förarna för konnektivitet betonades också den vaksamhet som krävs när det gäller användningen av de uppgifter som fås från fordon samt vikten av att följa lagstiftningen om skydd av personuppgifter. Utmaningen för varje berörd part är således att införliva dimensionen ”skydd av personuppgifter” från produkternas utformningsfas och se till att bilburna användare har insyn och kontroll när det gäller deras uppgifter i enlighet med skäl 78 i dataskyddsförordningen. Ett sådant tillvägagångssätt bidrar till att stärka användarnas förtroende och därmed den långsiktiga utvecklingen av denna teknik.

1.1 Relaterade texter

5. Uppkopplade fordon har blivit en viktig fråga för tillsynsmyndigheterna under det senaste årtiondet och ökat kraftigt under de senaste åren. Olika texter har därför publicerats på nationell och internationell nivå om säkerhet och integritet för uppkopplade fordon. Dessa föreskrifter och initiativ syftar till att komplettera de befintliga ramarna för dataskydd och integritet med sektorsspecifika regler eller ge vägledning till yrkesverksamma.

1.1.1 EU-initiativ och internationella initiativ

6. Sedan den 31 mars 2018 är ett 112-baserat eCall-system i fordon obligatoriskt för alla nya typer av fordon i kategorierna M1 och N1 (personbilar och lätta motorfordon)[4,5]. År 2006 hade artikel 29-arbetsgruppen redan antagit ett arbetsdokument om hur initiativet eCall påverkar uppgifts- och integritetsskyddet[6]. Som tidigare diskuterats antog artikel 29-arbetsgruppen dessutom ett yttrande i oktober 2017 om behandling av personuppgifter inom ramen för samverkande intelligenta transportsystem (C-ITS).

7. I januari 2017 offentliggjorde Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) en studie som fokuserade på it-säkerhet och motståndskraft hos smarta bilar, med en förteckning över känsliga tillgångar samt motsvarande hot, risker, begränsningsfaktorer och möjliga säkerhetsåtgärder att genomföra[7]. I september 2017 antog den internationella konferensen för ombudsmän för dataskydds- och integritetsfrågor (ICDPPC) en resolution

[3] Kampanjen ”My Car My Data”, http://www.mycarmydata.eu/.
[4] *The interoperable EU-wide eCall*, https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Europaparlamentets och rådets beslut nr 585/2014/EU av den 15 maj 2014 om införande av en interoperabel EU-omfattande eCall-tjänst (Text av betydelse för EES), https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014D0585.
[6] Arbetsdokument om hur initiativet eCall påverkar uppgifts- och integritetsskyddet, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_sv.pdf.
[7] *Cyber security and resilience of smart cars*, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

om uppkopplade fordon[8]. Slutligen antog även den internationella arbetsgruppen för dataskydd i telekommunikationer (IWGDPT) i april 2018 ett arbetsdokument om uppkopplade fordon[9].

1.1.2 Nationella initiativ från Europeiska dataskyddsstyrelsens ledamöter

8. I januari 2016 offentliggjorde *Datenschutzkonferenz* (den tyska dataskyddskonferensen) och *Verband der Automobilindustrie* (den tyska bilindustriföreningen) en gemensam förklaring om principerna för dataskydd i uppkopplade och ouppkopplade fordon[10]. I augusti 2017 offentliggjorde brittiska *Centre for Connected and Autonomous Vehicles* en handbok med principer för it-säkerhet för uppkopplade och automatiserade fordon i syfte att öka medvetenheten om denna fråga inom bilindustrin[11]. I oktober 2017 offentliggjorde den franska dataskyddsmyndigheten, *Commission Nationale de l'Informatique et des Libertés*, ett efterlevnadspaket för uppkopplade bilar för att hjälpa berörda parter att integrera inbyggt dataskydd och dataskydd som standard, så att registrerade får effektiv kontroll över sina uppgifter[12].

1.2 Tillämplig rätt

9. Den relevanta rättsliga ramen på EU-nivå är dataskyddsförordningen. Den är tillämplig i alla fall när behandling av uppgifter i samband med uppkopplade fordon innebär behandling av enskilda personers personuppgifter.

10. Utöver dataskyddsförordningen fastställs i direktiv 2002/58/EG, ändrat genom 2009/136/EG (*direktivet om integritet och elektronisk kommunikation*), **en särskild standard för alla aktörer som vill lagra eller få tillgång till information som lagras i en abonnents eller användares terminalutrustning i Europeiska ekonomiska samarbetsområdet (EES)**.

11. Merparten av bestämmelserna i direktivet om integritet och elektronisk kommunikation (artikel 6, artikel 9 osv.) gäller endast leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och leverantörer av allmänna kommunikationsnät, men artikel 5.3 är en allmän bestämmelse. Den är inte bara tillämplig på elektroniska kommunikationstjänster utan även på alla enheter, privata eller offentliga, som lagrar information på eller läser information från en terminalutrustning utan hänsyn till vilken typ av uppgifter som lagras eller görs tillgängliga.

---

[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.

[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.

12. Begreppet terminalutrustning definieras i direktiv 2008/63/EG[13]. I artikel 1 a definieras terminalutrustning som ”utrustning direkt eller indirekt ansluten till en nätanslutningspunkt i ett allmänt tillgängligt telenät för att sända, bearbeta eller ta emot information; i ettdera fallet (direkt eller indirekt) kan anslutningen göras med tråd, optisk fiber eller elektromagnetiskt; en anslutning är indirekt om utrustningen är placerad mellan terminalutrustningen och nätanslutningspunkten, b) jordstationsutrustning.”

13. Förutsatt att ovannämnda kriterier är uppfyllda bör därför det uppkopplade fordonet och den enhet som är ansluten till det betraktas som ”terminalutrustning” (precis som en dator, en smarttelefon eller en smart-tv), och bestämmelserna i artikel 5.3 i direktivet om integritet och elektronisk kommunikation ska tillämpas när så är relevant.

14. I enlighet med vad Europeiska dataskyddsstyrelsen angav i sitt yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och dataskyddsförordningen[14] föreskrivs i artikel 5.3 i direktivet att det i regel, och med förbehåll för de undantag från den regeln som anges i punkt 17 nedan, krävs tidigare samtycke för att få lagra information eller för att få tillgång till information som redan finns lagrad i en abonnents eller användares terminalutrustning. I den mån som informationen lagrad i slutanvändarens enhet utgör personuppgifter kommer artikel 5.3 i nämnda direktiv att ha företräde framför artikel 6 i dataskyddsförordningen i fråga om lagring av eller tillgång till denna information[15]. All behandling av personuppgifter efter ovannämnda behandling, bl.a. behandling av personuppgifter som erhållits genom tillgång till information i terminalutrustningen, måste ha en rättslig grund enligt artikel 6 i dataskyddsförordningen för att vara laglig[16].

15. Eftersom den personuppgiftsansvarige, när den begär samtycke till lagring av eller tillgång till information i enlighet med artikel 5.3 i direktivet om integritet och elektronisk kommunikation, måste informera den registrerade om alla ändamål med behandlingen – inklusive all behandling efter ovannämnda åtgärder (dvs. ”efterföljande behandling”) – är samtycke enligt artikel 6 i dataskyddsförordningen i allmänhet den lämpligaste rättsliga grunden för att omfatta behandlingen av personuppgifter efter sådana åtgärder (i den mån syftet med följande behandling förstås genom den registrerades samtycke, se punkterna 53–54 nedan). Samtycke kommer därför sannolikt att utgöra den rättsliga grunden både för lagring av och tillgång till information som redan lagras och för efterföljande behandling av personuppgifter[17]. Vid bedömningen av efterlevnaden av artikel 6 i dataskyddsförordningen bör man beakta att behandlingen som helhet omfattar specifika verksamheter för vilka

[13] Kommissionens direktiv 2008/63/EG av den 20 juni 2008 om konkurrens på marknaderna för teleterminalutrustning (kodifierad version) (Text av betydelse för EES), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A32008L0063.

[14] Europeiska dataskyddsstyrelsen, *Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter*, antaget den 12 mars 2019 (*yttrande 5/2019*), punkt 40.

[15] Se ovan, punkt 40.

[16] Se ovan, punkt 41.

[17] Samtycke som krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation och samtycke som krävs som rättslig grund för behandling av uppgifter (artikel 6 i dataskyddsförordningen) för samma specifika ändamål kan hämtas samtidigt (t.ex. genom att kryssa i en ruta som tydligt anger vad den registrerade samtycker till).

unionslagstiftaren har velat ge ytterligare skydd[18]. Dessutom måste personuppgiftsansvariga ta hänsyn till inverkan på registrerades rättigheter när de fastställer lämplig laglig grund för att respektera principen om rättvisa[19]. Slutsatsen är att personuppgiftsansvariga inte kan åberopa artikel 6 i dataskyddsförordningen för att minska det ytterligare skydd som föreskrivs i artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

16. Europeiska dataskyddsstyrelsen påminner om att begreppet samtycke i direktivet om integritet och elektronisk kommunikation är detsamma som begreppet samtycke i dataskyddsförordningen och måste uppfylla alla krav på samtycke enligt artiklarna 4.11 och 7 i dataskyddsförordningen.

17. Även om samtycke är principen ger artikel 5.3 i direktivet om integritet och elektronisk kommunikation möjlighet att undanta lagring av eller tillgång till information som redan finns lagrad i terminalutrustningen från kravet på informerat samtycke, om ett av följande kriterier uppfylls:

    - **Undantag 1:** Om det enda syftet är att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät.
    - **Undantag 2:** När det är absolut nödvändigt för att leverantören av en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt ska kunna tillhandahålla tjänsten.

18. I sådana fall grundar sig behandlingen av personuppgifter, inbegripet personuppgifter som erhålls genom tillgång till information i terminalutrustningen, på en av de rättsliga grunder som anges i artikel 6 i dataskyddsförordningen. Samtycke krävs exempelvis inte när behandling av uppgifter är nödvändig för att tillhandahålla GPS-navigationstjänster som den registrerade begär när sådana tjänster kan klassificeras som informationssamhällets tjänster.

1.3 Tillämpningsområde

19. Europeiska dataskyddsstyrelsen vill påpeka att dessa riktlinjer syftar till att underlätta efterlevnaden av den behandling av personuppgifter som utförs av ett stort antal aktörer som arbetar i denna miljö. De är dock inte avsedda att täcka alla typer av användning som är möjliga i detta sammanhang eller att ge vägledning för varje tänkbar specifik situation.

20. Detta dokument är särskilt inriktat på behandlingen av personuppgifter i samband med registrerades icke-yrkesmässiga användning av uppkopplade fordon, t.ex. förare, passagerare, fordonsägare, andra trafikanter osv. Mer specifikt handlar det om personuppgifter som i) behandlas inuti fordonet, ii) utbyts mellan fordonet och personliga apparater som är anslutna till det (t.ex. användarens smarttelefon) eller iii) samlas in lokalt i fordonet och exporteras till externa enheter (t.ex. fordonstillverkare, infrastrukturförvaltare, försäkringsbolag, bilverkstäder) för vidare behandling.

21. Definitionen av uppkopplat fordon måste ses som ett brett begrepp i detta dokument. Det kan definieras som ett fordon utrustat med många elektroniska styrenheter som är

[18] Yttrande 5/2019, punkt 41.

[19] Europeiska dataskyddsstyrelsen, *Riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade*, version 2.0, den 8 oktober 2019, punkt 1.

sammankopplade via ett fordonsbaserat nät samt anslutningsmöjligheter som gör det möjligt för det att dela information med andra anordningar både i och utanför fordonet. Därmed kan uppgifter utbytas mellan fordonet och de personliga enheter som är anslutna till det, t.ex. genom möjligheten att spegla mobilapplikationer till bilens inbyggda system för information och underhållning. Vidare omfattar detta dokument utvecklingen av fristående mobilapplikationer, dvs. applikationer som är oberoende av fordonet (t.ex. som endast kräver att smarttelefonen används), för att hjälpa förare eftersom de bidrar till fordonets anslutningskapacitet, även om de i praktiken kanske inte förlitar sig på överföring av uppgifter med fordonet i sig. Det finns många olika applikationer för uppkopplade fordon, som kan omfatta följande[20]:

22. *Rörlighetsstyrning:* Funktioner som gör det möjligt för förare att snabbt och på ett kostnadseffektivt sätt nå en destination genom att i god tid tillhandahålla information om GPS-navigering, potentiellt farliga miljöförhållanden (t.ex. isiga vägar), trafikstockningar eller vägbyggnadsarbeten, hjälp med parkeringsplats eller garage, optimerad bränsleförbrukning eller vägavgifter.

23. *Fordonshantering:* Funktioner som är avsedda att hjälpa förare att minska driftskostnaderna och förbättra användarvänligheten, såsom uppdateringar om fordonets skick och servicepåminnelser, överföring av användningsdata (t.ex. för fordonsreparationer), skräddarsydda, användningsbaserade försäkringar, fjärrmanövrering (t.ex. värmesystem) eller profilkonfigurationer (t.ex. stolinställning).

24. *Trafiksäkerhet:* Funktioner som varnar föraren för yttre faror och interna svar såsom krockskydd, varningssignaler, varningar vid avvikelse ur körfält, upptäckt av förartrötthet, nödanrop (eCall) eller ”svarta lådor” för olycksundersökning (färdregistrator).

25. *Underhållning:* Funktioner som informerar och underhåller förare och passagerare, såsom gränssnitt för smarttelefoner (handsfreesamtal, röstgenererade textmeddelanden), wifi-surfpunkter, musik, video, internet, sociala medier, mobila kontor eller ”smarta hem”-tjänster.

26. *Förarassistans:* Funktioner som omfattar helt eller delvis automatiserad körning, såsom körassistans eller autopilot vid intensiv trafik, parkering eller på motorvägar.

27. *Välbefinnande:* Funktioner som övervakar förarens komfort, förmåga och lämplighet att köra, såsom upptäckt av trötthet eller medicinsk hjälp.

28. Fordon kan därför vara direkt uppkopplade eller inte och personuppgifter kan samlas in på flera olika sätt, bland annat genom i) fordonssensorer, ii) telematikboxar eller iii) mobilapplikationer (som t.ex. kan nås från en enhet som tillhör en förare). För att omfattas av detta dokument måste mobilapplikationer vara kopplade till körmiljön. Applikationer för GPS-navigering omfattas till exempel. Applikationer vars funktioner endast föreslår intressanta platser (restauranger, historiska monument osv.) för föraren omfattas dock inte av dessa riktlinjer.

29. En stor del av de uppgifter som genereras av ett uppkopplat fordon avser en fysisk person som är identifierad eller kan identifieras, och utgör således personuppgifter. Uppgifterna omfattar t.ex. direkt identifierbara uppgifter (t.ex. förarens fullständiga identitet) samt

[20] PwC Strategy& 2014. *In the fast lane. The bright future of connected cars*, https://carrealtime.com/wp-content/uploads/2016/11/Strategyand_In-the-Fast-Lane.pdf.

indirekt identifierbara uppgifter såsom uppgifter om körningar som gjorts, uppgifter om användningen av fordonet (t.ex. om körstil eller tillryggalagd sträcka) eller fordonets tekniska uppgifter (t.ex. om slitage på fordonsdelar), som genom korshänvisningar till andra filer och särskilt fordonets identifieringsnummer kan kopplas till en fysisk person. Personuppgifter i uppkopplade fordon kan också omfatta metadata, t.ex. fordonets underhållsstatus. Med andra ord omfattas därför alla uppgifter som kan kopplas till en fysisk person av detta dokuments tillämpningsområde.

30. Det uppkopplade fordonets ekosystem omfattar ett brett spektrum av berörda parter. Detta ekosystem inbegriper mer specifikt traditionella aktörer inom bilindustrin liksom framväxande aktörer från den digitala industrin. Dessa riktlinjer riktar sig därför till fordonstillverkare, utrustningstillverkare och fordonsleverantörer, bilreparatörer, bilåterförsäljare, leverantörer av fordonstjänster, fordonsparksförvaltare, bilförsäkringsbolag, underhållningsleverantörer, teleoperatörer, väghållare och offentliga myndigheter samt registrerade. Europeiska dataskyddsstyrelsen understryker att kategorierna av registrerade kommer att skilja sig åt från en tjänst till en annan (t.ex. förare, ägare, passagerare osv.). Detta är en icke uttömmande förteckning eftersom ekosystemet omfattar en mängd olika tjänster, däribland tjänster för vilka direkt autentisering eller identifiering behövs och tjänster för vilka detta inte behövs.

31. Uppgiftsbehandling som utförs av fysiska personer i fordonet ”som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll” omfattas därför inte av dataskyddsförordningen[21]. Detta gäller särskilt användningen av personuppgifter i fordonen av de enda registrerade som angav sådana uppgifter i fordonets instrumentpanel. Europeiska dataskyddsstyrelsen erinrar dock om att enligt skäl 18 i dataskyddsförordningen är den ”tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet”.

1.3.1 Omfattas inte av detta dokument

32. Arbetsgivare som tillhandahåller tjänstebilar till sina anställda kan vilja övervaka den anställdes agerande (t.ex. för att garantera säkerheten för den anställde, varor eller fordon, fördela resurser, spåra och fakturera en tjänst eller kontrollera arbetstiden). Den uppgiftsbehandling som utförs av arbetsgivare i detta sammanhang väcker särskilda frågor om anställningsförhållanden, som kan regleras genom arbetslagstiftning på nationell nivå som inte kan specificeras i dessa riktlinjer[22].

33. Uppgiftsbehandling i samband med kommersiella fordon som används för yrkesmässiga ändamål (såsom kollektivtrafik) och delade transporter och mobilitetstjänster kan ge upphov till särskilda frågor som faller utanför dessa allmänna riktlinjers tillämpningsområde, men många av de principer och rekommendationer som anges här är också tillämpliga på dessa typer av behandling.

34. Eftersom uppkopplade fordon är radiobaserade system är de föremål för passiv spårning genom exempelvis wifi eller bluetooth. I den meningen skiljer de sig inte från andra anslutna enheter och omfattas av tillämpningsområdet för direktivet om integritet och elektronisk

[21] Se artikel 2.2 c i dataskyddsförordningen.
[22] Artikel 29-arbetsgruppen utvecklade detta i sitt WP 249-yttrande 2/2017 om behandling av personuppgifter på arbetsplatsen, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

kommunikation, som för närvarande håller på att ses över. Detta utesluter därför även storskalig spårning av wifi-utrustade fordon[23] genom ett tätt nät av personer i närheten som använder vanliga platstjänster för smarttelefoner. Dessa rapporterar rutinmässigt alla synliga wifi-nätverk till centrala servrar. Eftersom inbyggd wifi kan betraktas som en sekundär fordonsidentifierare[24] utgör detta en risk för systematisk kontinuerlig insamling av kompletta profiler över fordonsrörelser.

35. Fordon utrustas i allt högre grad med bildinspelningsutrustning (t.ex. backkameror eller bilkameror). Eftersom detta gäller frågan om att filma offentliga platser, vilket kräver en bedömning av den relevanta rättsliga ram som är specifik för varje medlemsstat, omfattas denna uppgiftsbehandling inte av dessa riktlinjer.

36. Uppgiftsbehandling som möjliggör samverkande intelligenta transportsystem (C-ITS), enligt definitionen i direktiv 2010/40/EU[25], har behandlats i ett särskilt yttrande från artikel 29-arbetsgruppen[26]. Definitionen av begreppet C-ITS i direktivet innehåller inga tekniska specifikationer, men artikel 29-arbetsgruppen fokuserar i sitt yttrande på kortdistanskommunikation, dvs. kommunikation utan inblandning av en nätoperatör. Mer specifikt analyserar den specifika användningsfall för initialt införande. Arbetsgruppen åtar sig också att i ett senare skede bedöma de nya frågor som utan tvekan kommer att väckas när högre automatiseringsnivåer införs. Eftersom C-ITS har mycket specifika konsekvenser för uppgiftsskyddet (oöverträffade mängder lokaliseringsuppgifter, kontinuerlig överföring av personuppgifter, utbyte av uppgifter mellan fordon och annan väginfrastruktur osv.) och detta fortfarande diskuteras på europeisk nivå omfattas behandlingen av personuppgifter i detta sammanhang inte av dessa riktlinjer.

37. Slutligen syftar detta dokument inte till att behandla alla tänkbara frågor som rör uppkopplade fordon och kan därför inte betraktas som uttömmande.

1.4 Definitioner

38. ***Behandling*** av personuppgifter omfattar alla åtgärder som inbegriper personuppgifter såsom insamling, registrering, organisering, strukturering, lagring, anpassning eller ändring, hämtning, läsning, användning, utlämnande genom överföring, spridning eller tillgängliggörande på annat sätt, sammanställning eller samkörning, begränsning, radering eller förstöring, osv[27].

[23] Läs mer här: 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 och Gerd Nolden, *Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings*, VEHICULAR 2017, Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, Frankrike, den 23–27 juli 2017, s. 32–37.

[25] Direktiv 2010/40/EU av den 7 juli 2020 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32010L0040.

[26] Artikel 29-arbetsgruppen, *Yttrande 03/2017 om behandling av personuppgifter inom ramen för samverkande intelligenta transportsystem (C-ITS)*, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

[27] Se artikel 4.2 i dataskyddsförordningen.

39. Den ***registrerade*** är den fysiska person som de uppgifter som behandlas avser. När det gäller uppkopplade fordon kan det i synnerhet vara föraren (huvudsaklig eller tillfällig), passageraren eller fordonets ägare[28].

40. Den **personuppgiftsansvarige** är den person som bestämmer ändamålen med och medlen för behandlingen i uppkopplade fordon[29]. Personuppgiftsansvariga kan innefatta tjänsteleverantörer som behandlar fordonsdata för att till föraren skicka trafikinformation, meddelanden om miljökörning eller varningar om fordonets funktion, försäkringsbolag som erbjuder användningsbaserade avtal eller fordonstillverkare som samlar in uppgifter om slitage som påverkar fordonets delar för att förbättra dess kvalitet. Enligt artikel 26 i dataskyddsförordningen kan två eller flera personuppgiftsansvariga gemensamt fastställa ändamålen med och medlen för behandlingen och därmed betraktas som gemensamt personuppgiftsansvariga. I detta fall måste de tydligt fastställa sina respektive skyldigheter, särskilt vad gäller utövandet av registrerades rättigheter och tillhandahållandet av den information som avses i artiklarna 13 och 14 i dataskyddsförordningen.

41. **Personuppgiftsbiträdet** är en person som behandlar personuppgifter för den personuppgiftsansvarige och för dennes räkning[30]. Personuppgiftsbiträdet samlar in och behandlar uppgifter på instruktioner från den personuppgiftsansvarige, utan att använda dessa uppgifter för egna ändamål. Exempelvis kan utrustningstillverkare och fordonsleverantörer i ett antal fall behandla uppgifter för fordonstillverkarnas räkning (vilket inte innebär att de inte kan vara personuppgiftsansvariga för andra ändamål). Utöver kravet på att personuppgiftsbiträden ska genomföra lämpliga tekniska och organisatoriska åtgärder för att garantera en säkerhetsnivå som är anpassad till riskerna fastställs personuppgiftsbiträdenas skyldigheter i artikel 28 i dataskyddsförordningen.

42. ***Mottagaren*** är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte[31]. Till exempel är en affärspartner till tjänsteleverantören som mottar personuppgifter som genererats av fordonet från tjänsteleverantören en mottagare av personuppgifter. Oavsett om dessa fungerar som ny personuppgiftsansvarig eller som personuppgiftsbiträde ska de uppfylla alla skyldigheter enligt dataskyddsförordningen.

43. Offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare[32]; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte. Brottsbekämpande myndigheter är till exempel behöriga tredje parter när de begär personuppgifter som en del av en utredning i enlighet med unionsrätten eller medlemsstaternas lagstiftning.

[28] Se artikel 4.1 i dataskyddsförordningen.
[29] Se artikel 4.7 i dataskyddsförordningen och Europeiska dataskyddsstyrelsen, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (*riktlinjerna 07/2020*).
[30] Se artikel 4.8 i dataskyddsförordningen och riktlinjerna 07/2020.
[31] Se artikel 4.9 i dataskyddsförordningen och riktlinjerna 07/2020.
[32] Se artikel 4.9 och skäl 31 i dataskyddsförordningen.

1.5 Risker för skyddet av integritet och personuppgifter

44. Artikel 29-arbetsgruppen har redan uttryckt flera farhågor om sakernas internet, som även kan tillämpas på uppkopplade fordon[33]. De frågor som rör datasäkerhet och kontroll över uppgifter som redan tagits upp avseende sakernas internet är ännu känsligare när det gäller uppkopplade fordon, eftersom de medför trafiksäkerhetsproblem – och kan påverka förarens fysiska integritet – i en miljö som traditionellt uppfattas som isolerad och skyddad från yttre inblandning.

45. Uppkopplade fordon ger också upphov till betydande oro för skyddet av personuppgifter och integritet i samband med behandlingen av lokaliseringsuppgifter, eftersom dess alltmer inkräktande karaktär kan försämra de nuvarande möjligheterna att förbli anonym. Europeiska dataskyddsstyrelsen vill lägga särskild tonvikt på och öka intressenternas medvetenhet om att användningen av lokaliseringsteknik kräver särskilda skyddsåtgärder för att förhindra övervakning av enskilda personer och missbruk av uppgifterna.

1.5.1 Bristande kontroll och informationsasymmetri

46. Fordonsförare och passagerare får inte alltid tillräcklig information om den behandling av uppgifter som äger rum i eller genom ett uppkopplat fordon. Informationen kanske endast lämnas till fordonsägaren, som kanske inte är föraren, och kanske inte heller lämnas i tid. Det finns således en risk för att otillräckliga funktioner eller alternativ erbjuds för att utöva den kontroll som krävs för att berörda personer ska kunna utnyttja sina rättigheter i fråga om skydd av personuppgifter och integritet. Detta är viktigt eftersom fordon under sin livstid kan tillhöra mer än en ägare, antingen för att de säljs eller för att de leasas snarare än köps.

47. Kommunikation i fordonet kan också utlösas automatiskt och som standard, utan att personen är medveten om detta. Om det inte finns någon möjlighet att faktiskt kontrollera hur fordonet och dess anslutna utrustning samverkar kommer det oundvikligen att bli oerhört svårt för användaren att kontrollera dataflödet. Det kommer att bli ännu svårare att kontrollera den efterföljande användningen av uppgifterna och därigenom förhindra eventuell funktionsglidning.

1.5.2 Kvaliteten på användarens samtycke

48. Europeiska dataskyddsstyrelsen understryker att när uppgiftsbehandlingen grundar sig på samtycke måste alla delar av ett giltigt samtycke uppfyllas, vilket innebär att samtycket ska vara frivilligt, specifikt och informerat och utgöra en otvetydig viljeyttring från den registrerade, i enlighet med tolkningen i Europeiska dataskyddsstyrelsens riktlinjer om samtycke[34]. Personuppgiftsansvariga måste noga se till att få giltigt samtycke från olika deltagare, t.ex. bilägare eller bilanvändare. Sådant samtycke ska tillhandahållas separat, för särskilda ändamål och får inte inbakas i ett avtal för att köpa eller leasa en ny bil. Samtycket måste kunna återkallas lika lätt som det ges.

49. Detsamma måste tillämpas när samtycke krävs för att följa direktivet om integritet och elektronisk kommunikation, t.ex. vid lagring av eller tillgång till information som redan finns lagrad i fordonet, vilket krävs i vissa fall enligt artikel 5.3 i direktivet om integritet och

[33] Artikel 29-arbetsgruppen, *Yttrande 08/2014 om den senaste utvecklingen av sakernas internet*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_sv.pdf.
[34] Europeiska dataskyddsstyrelsen, *Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679*, version 1.1, den 4 maj 2020 (*riktlinjerna 05/2020*).

elektronisk kommunikation. Såsom anges ovan måste samtycke i detta sammanhang tolkas mot bakgrund av dataskyddsförordningen.

50. I många fall är användaren kanske inte medveten om den uppgiftsbehandling som utförs i hans eller hennes fordon. Sådan brist på information utgör ett betydande hinder för att visa att giltigt samtycke har getts enligt dataskyddsförordningen, eftersom samtycket måste vara informerat. Under sådana omständigheter kan samtycke inte åberopas som rättslig grund för motsvarande uppgiftsbehandling enligt dataskyddsförordningen.

51. Klassiska mekanismer som används för att inhämta enskilda personers samtycke kan vara svåra att tillämpa inom ramen för uppkopplade fordon, vilket leder till ett ”lågkvalitativt” samtycke som grundar sig på brist på information eller på den faktiska omöjligheten att ge finjusterat samtycke i enlighet med de preferenser som uttrycks av enskilda personer. I praktiken kan det också vara svårt att inhämta samtycke för förare och passagerare som inte har någon koppling till fordonets ägare när det gäller begagnade, leasade, hyrda eller lånade fordon.

52. När direktivet om integritet och elektronisk kommunikation inte kräver den registrerades samtycke har den personuppgiftsansvarige ändå ansvaret för att välja den rättsliga grund enligt artikel 6 i dataskyddsförordningen som är mest lämplig för behandlingen av personuppgifter.

1.5.3 Ytterligare behandling av personuppgifter

53. När uppgifter samlas in på grundval av samtycke i enlighet med artikel 5.3 i direktivet om integritet och elektronisk kommunikation eller ett av undantagen i artikel 5.3, och därefter behandlas i enlighet med artikel 6 i dataskyddsförordningen, kan de endast behandlas ytterligare antingen om den personuppgiftsansvarige begär ytterligare samtycke för detta andra ändamål eller om den personuppgiftsansvarige kan visa att behandlingen grundar sig på unionsrätten eller en medlemsstats lagstiftning för att skydda de mål som avses i artikel 23.1 i dataskyddsförordningen[35]. Europeiska dataskyddsstyrelsen anser att ytterligare behandling på grundval av ett förenlighetstest enligt artikel 6.4 i dataskyddsförordningen inte är möjlig i sådana fall, eftersom det skulle undergräva standarden för dataskydd i direktivet om integritet och elektronisk kommunikation. Samtycke måste, när så krävs enligt direktivet om integritet och elektronisk kommunikation, vara specifikt och informerat, vilket innebär att de registrerade måste vara medvetna om varje behandlingssyfte och ha rätt att vägra specifika syften[36]. Om ytterligare behandling på grundval av ett förenlighetstest enligt artikel 6.4 i dataskyddsförordningen skulle vara möjlig skulle själva principen för samtyckeskraven i det nuvarande direktivet kringgås.

54. Europeiska dataskyddsstyrelsen erinrar om att det första samtycket aldrig kommer att legitimera ytterligare behandling eftersom samtycket måste vara informerat och specifikt för att vara giltigt.

55. Till exempel får telemetridata som samlas in för underhållsändamål under användning av fordonet inte lämnas ut till bilförsäkringsbolag utan användarnas samtycke i syfte att skapa förarprofiler för att erbjuda försäkringar baserade på körbeteende.

[35] Se även Europeiska dataskyddsstyrelsen, *Guidelines 10/2020 on restrictions under Article 23 GDPR*.
[36] Riktlinjerna 05/2020, avsnitt 3.2 och 3.3.

56. Dessutom får brottsbekämpande myndigheter behandla uppgifter som samlas in av uppkopplade fordon för att upptäcka fortkörning eller andra överträdelser om och när de särskilda villkoren i brottsbekämpningsdirektivet är uppfyllda. I detta fall kommer sådana uppgifter att anses röra fällande domar i brottmål och lagöverträdelser som innefattar brott enligt villkoren i artikel 10 i dataskyddsförordningen och tillämplig nationell lagstiftning. Tillverkarna får förse brottsbekämpande myndigheter med sådana uppgifter om de särskilda villkoren för sådan behandling är uppfyllda. Europeiska dataskyddsstyrelsen påpekar att behandling av personuppgifter som endast sker i syfte att tillmötesgå brottsbekämpande myndigheters begäranden inte utgör ett särskilt, uttryckligt angivet och berättigat ändamål i den mening som avses i artikel 5.1 b i dataskyddsförordningen. När så är tillåtet enligt lag kan brottsbekämpande myndigheter vara tredje parter i den mening som avses i artikel 4.10 i dataskyddsförordningen. I detta fall skulle tillverkarna ha rätt att förse dem med alla uppgifter som de har tillgång till, förutsatt att den relevanta rättsliga ramen i varje medlemsstat följs.

1.5.4 Överdriven datainsamling

57. Med det ständigt ökande antalet sensorer som används i uppkopplade fordon finns det en mycket stor risk för överdriven datainsamling jämfört med vad som är nödvändigt för att uppnå syftet.

58. Utvecklingen av nya funktioner, särskilt sådana som bygger på algoritmer för maskininlärning, kan kräva en stor mängd data som samlas in under lång tid.

1.5.5 Säkerhet för personuppgifter

59. Den stora mängden funktioner, tjänster och gränssnitt (t.ex. internet, usb, RFID, wifi) som erbjuds av uppkopplade fordon ökar attackytan och därmed antalet potentiella sårbarheter genom vilka personuppgifter kan äventyras. Till skillnad från de flesta apparater inom sakernas internet är uppkopplade fordon kritiska system där en säkerhetsöverträdelse kan innebära en fara för användarnas och andra människors liv. Det är därför allt viktigare att ta itu med risken för hackare som försöker utnyttja de uppkopplade fordonens sårbarhet.

60. Dessutom måste personuppgifter som lagras i fordon och/eller på externa platser (t.ex. i molninfrastrukturer) vara tillräckligt skyddade mot obehörig åtkomst. Vid underhåll måste till exempel fordonet överlämnas till en tekniker som kommer att behöva tillgång till vissa av fordonets tekniska uppgifter. Även om teknikern måste ha tillgång till de tekniska uppgifterna finns det en möjlighet att teknikern kan försöka få tillgång till alla uppgifter som lagras i fordonet.

2 ALLMÄNNA REKOMMENDATIONER

61. För att minska de risker för registrerade som anges ovan bör följande allmänna rekommendationer följas av tillverkare av fordon och utrustning, tjänsteleverantörer eller andra berörda parter som kan fungera som personuppgiftsansvarig eller personuppgiftsbiträde i samband med uppkopplade fordon.

2.1 Kategorier av uppgifter

62. Som påpekades i inledningen kommer de flesta uppgifter som rör uppkopplade fordon att betraktas som personuppgifter i den mån det är möjligt att koppla dem till en eller flera identifierbara personer. Detta inbegriper tekniska uppgifter om fordonets rörelse (t.ex.

hastighet, tillryggalagd sträcka) och fordonets skick (t.ex. motorns kylvätsketemperatur, motorns varvtal, däcktryck). Vissa uppgifter som genereras av uppkopplade fordon kan också kräva särskild uppmärksamhet på grund av deras känslighet och/eller potentiella inverkan på de registrerades rättigheter och intressen. För närvarande har Europeiska dataskyddsstyrelsen identifierat tre kategorier av personuppgifter som kräver särskild uppmärksamhet från tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga: lokaliseringsuppgifter, biometriska uppgifter (och särskilda kategorier av uppgifter enligt definitionen i artikel 9 i dataskyddsförordningen) och uppgifter som kan avslöja brott eller trafiköverträdelser.

2.1.1 Lokaliseringsuppgifter

63. Vid insamling av personuppgifter bör tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga ha i åtanke att lokaliseringsuppgifter särskilt avslöjar de registrerades levnadsvanor. De resor som genomförs är mycket karakteristiska, eftersom de gör det möjligt att utläsa förarens arbetsplats och hem liksom platser för intresse (fritid). Resorna kan även eventuellt avslöja känslig information såsom religion genom gudstjänstlokaler eller sexuell läggning genom de besökta platserna. Tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga bör därför särskilt se till att inte samla in lokaliseringsuppgifter, utom när detta är absolut nödvändigt för ändamålet med behandlingen. Som exempel kan nämnas att när behandlingen består i att avkänna fordonets rörelse är gyroskopet tillräckligt för att fylla denna funktion, utan att det är nödvändigt att samla in lokaliseringsuppgifter.

64. I allmänhet omfattas insamling av lokaliseringsuppgifter också av följande principer:

- Lämplig konfiguration av hur ofta insamlade lokaliseringsuppgifter är tillgängliga och hur detaljerade de är i förhållande till ändamålet med behandlingen. Exempelvis bör en väderapplikation inte kunna komma åt fordonets position varje sekund, ens med den registrerades samtycke.

- Tillhandahållande av korrekt information om ändamålet med behandlingen (lagras t.ex. platshistorik? Om så är fallet, vad är syftet med det?).

- När behandlingen grundar sig på samtycke, erhållande av giltigt (frivilligt, specifikt och informerat) samtycke som skiljer sig från de allmänna försäljnings- eller användningsvillkoren, t.ex. för fordonsdatorn.

- Aktivering av plats endast när användaren startar en funktion som kräver att fordonets position är känd, och inte som standard och kontinuerligt när bilen startas.

- Information till användaren om att platsen har aktiverats, särskilt genom användning av ikoner (t.ex. en pil som rör sig över skärmen).

- Möjlighet att när som helst avaktivera platsen.

- Fastställande av en begränsad lagringsperiod.

2.1.2 Biometriska uppgifter

65. När det gäller uppkopplade fordon får biometriska uppgifter som används för att unikt identifiera en fysisk person behandlas, inom ramen för artikel 9 i dataskyddsförordningen och de nationella undantagen, bland annat för att möjliggöra åtkomst till ett fordon, autentisera föraren/ägaren och/eller möjliggöra åtkomst till en förares profilinställningar

och preferenser. När man överväger att använda biometriska uppgifter innebär garantin för att den registrerade har full kontroll över sina uppgifter å ena sidan att det finns ett icke-biometriskt alternativ (t.ex. att en fysisk nyckel eller en kod kan användas) utan ytterligare begränsningar (dvs. det bör inte vara obligatoriskt att använda biometriska uppgifter), och, å andra sidan, att den biometriska mallen lagras och jämförs i krypterad form och endast på lokal nivå, där de biometriska uppgifterna inte behandlas av en extern läsar- eller jämförelseterminal.

66. När det gäller biometriska uppgifter[37] är det viktigt att säkerställa att lösningen för biometrisk autentisering är tillräckligt tillförlitlig, särskilt genom att följa följande principer:

- Den biometriska lösning som används (t.ex. andelen felaktig positiv och felaktig negativ identifiering) anpassas till säkerhetsnivån för den erfordrade åtkomstkontrollen.
- Den biometriska lösning som används bygger på en sensor som är motståndskraftig mot attacker (t.ex. användning av ett platt fingeravtryck för igenkänning av fingeravtryck).
- Antalet autentiseringsförsök är begränsat.
- Den biometriska mallen/modellen lagras i fordonet i krypterad form med hjälp av en kryptografisk algoritm och nyckelhantering som överensstämmer med den senaste tekniken.
- Rådata som används för att fylla i den biometriska mallen och för användarautentisering behandlas i realtid utan att någonsin lagras, ens lokalt.

2.1.3 Uppgifter som avslöjar brott eller andra överträdelser

67. För att behandla uppgifter som rör potentiella brott i den mening som avses i artikel 10 i dataskyddsförordningen rekommenderar Europeiska dataskyddsstyrelsen att man använder sig av lokal behandling av uppgifterna där den registrerade har full kontroll över behandlingen i fråga (se diskussionen om lokal behandling i avsnitt 2.4). Förutom vid vissa undantag (se fallstudien om olycksundersökningar som presenteras nedan i avsnitt 3.3) är extern behandling av uppgifter som avslöjar brott eller andra överträdelser förbjuden. Beroende på uppgifternas känslighet måste det därför vidtas kraftfulla säkerhetsåtgärder, såsom de som beskrivs i avsnitt 2.7, för att erbjuda skydd mot orättmätig åtkomst, ändring och radering av dessa uppgifter.

68. Vissa kategorier av personuppgifter från uppkopplade fordon skulle kunna visa att ett brott eller en annan överträdelse har begåtts eller håller på att begås (”brottsrelaterade uppgifter”) och därför omfattas av särskilda restriktioner (t.ex. uppgifter som visar att fordonet korsade en vit linje, ett fordons momentana hastighet kombinerat med exakta lokaliseringsuppgifter). Om sådana uppgifter skulle behandlas av de behöriga nationella myndigheterna för brottsutredning och lagföring av brott skulle i synnerhet de skyddsåtgärder som föreskrivs i artikel 10 i dataskyddsförordningen vara tillämpliga.

2.2 Ändamål

69. Personuppgifter får behandlas för en rad olika ändamål som rör uppkopplade fordon, däribland förarsäkerhet, försäkring, effektiv transport, underhållning eller informationstjänster. I enlighet med dataskyddsförordningen måste personuppgiftsansvariga säkerställa att deras ändamål är ”särskilda, uttryckligt angivna och

[37] Den princip om förbud som fastställs i artikel 9.1 i dataskyddsförordningen avser endast ”biometriska uppgifter för att entydigt identifiera en fysisk person”.

berättigade", inte senare behandlas på ett sätt som är oförenligt med dessa ändamål och att det finns en giltig rättslig grund för behandlingen i enlighet med artikel 5 i dataskyddsförordningen. Några konkreta exempel på ändamål som kan eftersträvas av personuppgiftsansvariga som arbetar i sammanhang av uppkopplade fordon diskuteras i del III av dessa riktlinjer, tillsammans med särskilda rekommendationer för varje typ av behandling.

2.3 Relevans och uppgiftsminimering

70. För att uppfylla principen om uppgiftsminimering[38] bör tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga ägna särskild uppmärksamhet åt de uppgiftskategorier som de behöver från ett uppkopplat fordon, eftersom de endast ska samla in personuppgifter som är relevanta och nödvändiga för behandlingen. Exempelvis är lokaliseringsuppgifter särskilt inkräktande och kan avslöja många av de registrerades levnadsvanor. Därför bör branschaktörerna särskilt se till att inte samla in lokaliseringsuppgifter, såvida det inte är absolut nödvändigt för behandlingen (se diskussionen om lokaliseringsuppgifter ovan i avsnitt 2.1).

2.4 Inbyggt dataskydd och dataskydd som standard

71. Med beaktande av de många olika personuppgifter som produceras av uppkopplade fordon noterar Europeiska dataskyddsstyrelsen att personuppgiftsansvariga är skyldiga att säkerställa att teknik som används i samband med uppkopplade fordon konfigureras för att respektera enskilda personers integritet genom att tillämpa skyldigheterna avseende inbyggt dataskydd och dataskydd som standard i enlighet med artikel 25 i dataskyddsförordningen. Tekniken bör utformas för att minimera insamlingen av personuppgifter, tillhandahålla standardinställningar som skyddar integriteten och säkerställa att de registrerade är välinformerade och har möjlighet att enkelt ändra konfigurationer som rör deras personuppgifter. Särskild vägledning om hur tillverkare och tjänsteleverantörer kan uppfylla principen om inbyggt dataskydd och dataskydd som standard skulle kunna vara till nytta för branschen och tredjepartsleverantörer av applikationer.

72. Vissa allmänna förfaranden, som beskrivs nedan, kan också bidra till att minska riskerna för fysiska personers rättigheter och friheter med anknytning till uppkopplade fordon[39].

2.4.1 Lokal behandling av personuppgifter

73. I allmänhet bör tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga när så är möjligt använda sig av processer som inte inbegriper personuppgifter eller överföring av personuppgifter utanför fordonet (dvs. uppgifterna behandlas internt). Uppkopplade fordons beskaffenhet medför dock risker, t.ex. för attacker på lokal behandling av externa aktörer eller att lokala uppgifter läcker ut genom att delar av fordonet säljs. Därför bör lämpliga resurser och säkerhetsåtgärder beaktas för att säkerställa att lokal behandling förblir lokal. Detta scenario har fördelen att användaren garanteras ensam och fullständig kontroll över sina personuppgifter, och därmed medför det på ett inbyggt sätt mindre integritetsrisker, särskilt genom att förbjuda uppgiftsbehandling av berörda parter utan den registrerades vetskap. Det möjliggör också behandling av känsliga uppgifter, såsom biometriska uppgifter eller uppgifter som rör brott eller andra

[38] Artikel 5.1 c i dataskyddsförordningen.
[39] Se även Europeiska dataskyddsstyrelsen, *Riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard*, version 2.0, antagna den 20 oktober 2020 (*riktlinjerna 4/2019*).

överträdelser, samt detaljerade lokaliseringsuppgifter som annars skulle omfattas av strängare regler (se nedan). På samma sätt medför det färre it-säkerhetsrisker och har liten latens, vilket gör det särskilt lämpligt för automatiserad förarassistans. Några exempel på denna typ av lösning kan vara följande:

- Applikationer för miljökörning som behandlar data i fordonet för att visa råd om miljökörning i realtid på fordonets skärm.

- Applikationer som innebär överföring av personuppgifter till en enhet såsom en smarttelefon under användarens fulla kontroll (via exempelvis bluetooth eller wifi) och där fordonets uppgifter inte överförs till applikationsleverantörerna eller fordonstillverkarna. Detta skulle till exempel omfatta parkoppling av smarttelefoner för att använda bilens bildskärm, multimediasystem, mikrofon (eller andra sensorer) för telefonsamtal osv., i den mån de insamlade uppgifterna fortfarande kontrolleras av den registrerade och uteslutande används för att tillhandahålla den begärda tjänsten.

- Applikationer som ökar säkerheten i fordonet, t.ex. avger ljudsignaler eller vibrationer på ratten när en förare kör om en bil utan att blinka eller kör över vita linjer, eller ger varningar om fordonets skick (t.ex. en varning om slitage som påverkar bromsklossarna).

- Applikationer för att låsa upp, starta och/eller aktivera vissa fordonskommandon med hjälp av förarens biometriska uppgifter som lagras inuti fordonet (såsom ansikts- eller talmodeller eller detaljerna (s.k. minutiae) i ett fingeravtryck).

74. Ovannämnda applikationer omfattar behandling som utförs för att en fysisk person ska kunna utöva verksamhet av rent privat natur (dvs. utan överföring av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde). I enlighet med artikel 2.2 i dataskyddsförordningen **faller dessa applikationer därför utanför dataskyddsförordningens tillämpningsområde.**

75. Om dataskyddsförordningen inte är tillämplig på behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll är den emellertid tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet (biltillverkare, tjänsteleverantörer osv.) i enlighet med skäl 18 i dataskyddsförordningen. När de fungerar som personuppgiftsansvariga eller personuppgiftsbiträden måste de därför utveckla säkra bilapplikationer, med vederbörlig respekt för principen om inbyggt integritetsskydd och integritetsskydd som standard. Enligt skäl 78 i dataskyddsförordningen gäller i samtliga fall följande: ”Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd.”[40] Å ena sidan kommer det att främja utvecklingen av användarcentrerade tjänster och å andra sidan kommer det att underlätta och säkra all vidare användning i framtiden som skulle kunna falla tillbaka inom

[40] Se även riktlinjerna 4/2019 för ytterligare rekommendationer om inbyggt integritetsskydd och integritetsskydd som standard.

dataskyddsförordningens tillämpningsområde. Mer specifikt rekommenderar Europeiska dataskyddsstyrelsen att man utvecklar en säker applikationsplattform i bilen som är fysiskt skild från säkerhetsrelevanta bilfunktioner, så att tillgången till bilens uppgifter inte är beroende av onödig extern molnkapacitet.

76. Fordonstillverkare och tjänsteleverantörer bör när så är möjligt överväga lokal databehandling för att minska de potentiella riskerna med molnbehandling, vilket betonas i artikel 29-arbetsgruppens yttrande om datormoln[41].

77. I allmänhet bör användarna kunna kontrollera hur deras uppgifter samlas in och behandlas i fordonet:

- Information om behandlingen måste ges på förarens språk (instruktionsbok, inställningar osv.).
- Europeiska dataskyddsstyrelsen rekommenderar att endast uppgifter som är absolut nödvändiga för fordonets funktion behandlas som standard. Registrerade bör ha möjlighet att aktivera eller avaktivera uppgiftsbehandlingen för varje annat ändamål och personuppgiftsansvarig/personuppgiftsbiträde och ha möjlighet att radera de berörda uppgifterna, med beaktande av ändamålet och den rättsliga grunden för behandlingen.
- Uppgifter bör inte överföras till någon tredje part (dvs. användaren har ensam tillgång till uppgifterna).
- Uppgifterna bör lagras endast så länge som det är nödvändigt för tillhandahållandet av tjänsten eller när så krävs av andra skäl enligt unionsrätten eller medlemsstaternas lagstiftning.
- Registrerade bör kunna radera alla personuppgifter permanent innan fordonet bjuds ut till försäljning.
- Registrerade bör, där så är möjligt, ha direkt tillgång till de uppgifter som genereras av dessa applikationer.

78. Slutligen kan ”hybridbehandling” ofta införas, eftersom det kanske inte alltid är möjligt att använda lokal databehandling för varje användningsfall. Exempelvis kan personuppgifter om körbeteende (såsom kraften på bromspedalen, körsträcka osv.) inom ramen för en användarbaserad försäkring antingen behandlas inne i fordonet eller av leverantören av telematiktjänster för försäkringsbolagets (den personuppgiftsansvariges) räkning för att ge numeriska poäng som överförs till försäkringsbolaget på fastställd basis (t.ex. månadsvis). På så sätt får försäkringsbolaget inte tillgång till rådata om beteende utan endast till det sammanlagda poängtal som är resultatet av behandlingen. Detta säkerställer att principerna om uppgiftsminimering uppfylls genom konstruktionen. Detta innebär också att användarna måste ha möjlighet att utöva sina rättigheter när uppgifter lagras av andra parter. En användare bör till exempel ha möjlighet att radera uppgifter som finns lagrade i en bilverkstads eller bilhandlares system enligt villkoren i artikel 17 i dataskyddsförordningen.

[41] Artikel 29-arbetsgruppen, *Yttrande 5/2012 om datormoln (cloud computing)*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_sv.pdf.

2.4.2 Anonymisering och pseudonymisering

79. Om överföring av personuppgifter utanför fordonet planeras bör man överväga att anonymisera dem innan de överförs. Vid anonymiseringen bör den personuppgiftsansvarige ta hänsyn till all behandling som kan leda till avanonymisering av uppgifter, såsom överföring av lokalt anonymiserade uppgifter. Europeiska dataskyddsstyrelsen påminner om att principerna för dataskyddet inte gäller för anonym information, dvs. information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar[42]. När en datauppsättning verkligen är anonymiserad och enskilda personer inte längre kan identifieras gäller inte längre EU:s dataskyddslagstiftning. Som en följd av detta kan anonymisering, där så är relevant, vara en bra strategi för att behålla fördelarna och minska riskerna i samband med uppkopplade fordon.

80. Såsom anges i yttrandet från artikel 29-arbetsgruppen om avidentifieringsmetoder kan olika metoder användas – ibland i kombination – för att uppnå anonymisering av uppgifter[43].

81. Andra metoder, såsom pseudonymisering[44], kan bidra till att minimera de risker som uppgiftsbehandlingen ger upphov till, med beaktande av att direkt identifierbara uppgifter i de flesta fall inte är nödvändiga för att uppnå syftet med behandlingen. Pseudonymisering, om den förstärks genom säkerhetsåtgärder, förbättrar skyddet av personuppgifter genom att minska riskerna för missbruk. Pseudonymisering är reversibel, till skillnad från anonymisering, och pseudonymiserade uppgifter betraktas som personuppgifter som omfattas av dataskyddsförordningen.

2.4.3 Konsekvensbedömning avseende dataskydd

82. Med tanke på omfattningen av och känsligheten hos de personuppgifter som kan genereras via uppkopplade fordon är det troligt att behandling – särskilt i situationer där personuppgifter behandlas utanför fordonet – ofta leder till att enskilda personers rättigheter och friheter utsätts för hög risk. Om så är fallet kommer branschaktörer att vara skyldiga att utföra en konsekvensbedömning avseende dataskydd för att identifiera och minska riskerna i enlighet med artiklarna 35 och 36 i dataskyddsförordningen. Även i de fall där en konsekvensbedömning avseende dataskydd inte krävs är det bästa praxis att genomföra en sådan så tidigt som möjligt i utformningsprocessen. Detta kommer att göra det möjligt för branschaktörerna att beakta resultaten av denna analys i sina utformningsval innan ny teknik tas i bruk.

2.5 Upplysningar

83. Före behandlingen av personuppgifter ska den registrerade informeras om den personuppgiftsansvariges identitet (t.ex. tillverkaren av fordonet och utrustningen eller tjänsteleverantören), syftet med behandlingen, uppgiftsmottagarna, den period under

[42] Se artikel 4.1 och skäl 26 i dataskyddsförordningen.
[43] Artikel 29-arbetsgruppen, *Yttrande 05/2014 om avidentifieringsmetoder*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sv.pdf.
[44] Artikel 4.5 i dataskyddsförordningen. Enisas rapport av den 3 december 2019. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

vilken uppgifterna kommer att lagras och den registrerades rättigheter enligt dataskyddsförordningen[45].

84. Tillverkaren av fordon och utrustning, tjänsteleverantören eller annan personuppgiftsansvarig bör dessutom ge den registrerade följande information på ett tydligt, enkelt och lättillgängligt sätt:

- Kontaktuppgifter till dataskyddsombudet.
- Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
- Uttryckligt omnämnande av den personuppgiftsansvariges eller tredje parts berättigade intressen, när sådana berättigade intressen utgör den rättsliga grunden för behandlingen.
- Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
- Denna rätt att när som helst återkalla samtycket utan att detta påverkar lagligheten av behandling som grundar sig på samtycke, innan detta återkallas, om behandlingen grundar sig på samtycke.
- I tillämpliga fall, det faktum att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och skyddsåtgärder som används för att överföra dem.
- Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
- Förekomsten av automatiserat beslutsfattande, inbegripet profilering som har rättsliga följder för den registrerade eller på liknande sätt i betydande grad påverkar den registrerade samt meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade. Detta skulle särskilt kunna vara fallet vid tillhandahållande av användningsbaserade försäkringar till enskilda personer.
- Rätten att inge klagomål till en tillsynsmyndighet.
- Information om ytterligare behandling.
- Vid gemensamt personuppgiftsansvar, tydlig och fullständig information om varje personuppgiftsansvarigs ansvar.

[45] Artiklarna 5.1 a och 13 i dataskyddsförordningen. Se även artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679* (wp260rev.01), godkända av Europeiska dataskyddsstyrelsen.

85. I vissa fall samlas personuppgifter inte in direkt från den berörda personen. En tillverkare av fordon och utrustning kan till exempel anlita en återförsäljare för att samla in information om fordonets ägare för att erbjuda en tjänst för akut vägassistans. Om uppgifter inte har samlats in direkt ska tillverkaren av fordon och utrustning, tjänsteleverantören eller annan personuppgiftsansvarig utöver den information som nämns ovan även ange vilka kategorier av personuppgifter som berörs, varifrån personuppgifterna kommer och, i tillämpliga fall, om dessa uppgifter kommer från offentligt tillgängliga källor. Informationen måste tillhandahållas av den personuppgiftsansvarige inom rimlig tid efter det att uppgifterna erhållits, och **senast vid det första av följande datum** i enlighet med artikel 14.3 i dataskyddsförordningen: i) en månad efter det att uppgifterna erhållits, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas, ii) vid tidpunkten för den första kommunikationen med den registrerade, eller iii) om uppgifterna överförs till en tredje part, innan uppgifterna överförs.

86. Nya uppgifter kan också behöva lämnas till registrerade när de hanteras av en ny personuppgiftsansvarig. En vägassistanstjänst som interagerar med uppkopplade fordon kan tillhandahållas av olika personuppgiftsansvariga beroende på i vilket land eller region assistansen behövs. Nya personuppgiftsansvariga bör ge registrerade den information som krävs när de registrerade passerar gränser och när tjänster som interagerar med uppkopplade fordon tillhandahålls av nya personuppgiftsansvariga.

87. Informationen till de registrerade kan tillhandahållas i skikt[46], dvs. genom att man skiljer mellan två informationsnivåer: å ena sidan information på primär nivå, som är den viktigaste för de registrerade, och å andra sidan information som förmodligen är av intresse i ett senare skede. Den viktiga informationen på primär nivå omfattar, utöver den personuppgiftsansvariges identitet, syftet med behandlingen och en beskrivning av den registrerades rättigheter samt eventuell ytterligare information om den behandling som har störst inverkan på den registrerade och behandling som skulle kunna överraska den registrerade. Europeiska dataskyddsstyrelsen rekommenderar att den registrerade, när det gäller uppkopplade fordon, görs uppmärksam på alla mottagare i det första informationsskiktet. Såsom anges i artikel 29-arbetsgruppens riktlinjer om öppenhet bör personuppgiftsansvariga tillhandahålla information om de mottagare som är mest meningsfull för de registrerade. I praktiken är detta mottagarnas namn, så att de registrerade vet exakt vem som har deras personuppgifter. Om de personuppgiftsansvariga inte kan uppge mottagarnas namn bör informationen vara så specifik som möjligt och innehålla uppgift om typen av mottagare (dvs. med hänvisning till den verksamhet som denne bedriver), bransch, sektor, undersektor och mottagarnas belägenhet.

88. De registrerade kan informeras genom kortfattade och lättförståeliga klausuler i avtalet om försäljning av fordonet, i avtalet om tillhandahållande av tjänster och/eller i något annat skriftligt medium, med hjälp av separata dokument (t.ex. fordonets underhållsjournal eller instruktionsbok) eller fordonsdatorn.

89. Standardiserade symboler skulle kunna användas utöver den information som krävs enligt artiklarna 13 och 14 i dataskyddsförordningen för att öka transparensen genom att potentiellt minska behovet av stora mängder skriftlig information som ska presenteras för den registrerade. Den bör vara synlig i fordon så att den, i förhållande till den planerade

[46] Se artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679* (wp260rev.01), godkända av Europeiska dataskyddsstyrelsen.

behandlingen, ger en god överblick som är begriplig och tydligt läsbar. Europeiska dataskyddsstyrelsen betonar vikten av att standardisera dessa symboler så att användaren hittar samma symboler oavsett fordonets märke eller modell. När vissa typer av uppgifter samlas in, t.ex. plats, skulle fordonen till exempel kunna ha en tydlig signal ombord (t.ex. en lampa inuti fordonet) för att informera passagerarna om uppgiftsinsamlingen.

2.6 Den registrerades rättigheter

90. Tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga bör underlätta de registrerades kontroll över sina uppgifter under hela behandlingsperioden genom att införa särskilda verktyg som gör det möjligt att på ett effektivt sätt utöva sina rättigheter, särskilt rätten till tillgång, rättelse, radering, rätten att begränsa behandlingen och, beroende på den rättsliga grunden för behandlingen, rätten till dataportabilitet och till att göra invändningar.

91. För att underlätta ändringar av inställningarna bör ett profilhanteringssystem införas för att lagra kända förares preferenser och hjälpa dem att enkelt ändra sina sekretessinställningar när som helst. Systemet för profilhantering bör centralisera alla datainställningar för varje uppgiftsbehandling, särskilt för att underlätta åtkomst, radering, borttagning och portabilitet av personuppgifter från fordonssystem på den registrerades begäran. Förarna bör ha möjlighet att när som helst tillfälligt eller permanent stoppa insamlingen av vissa typer av uppgifter, såvida det inte finns en särskild rättslig grund som den personuppgiftsansvarige kan anföra för att fortsätta insamlingen av specifika uppgifter. När ett avtal erbjuder ett personligt erbjudande baserat på körbeteende kan detta innebära att användaren till följd av detta åter bör omfattas av standardvillkoren i det avtalet. Dessa funktioner bör införas inuti fordonet, även om de också skulle kunna tillhandahållas de registrerade på andra sätt (t.ex. genom en särskild applikation). För att göra det möjligt för registrerade att snabbt och enkelt ta bort personuppgifter som kan lagras i bilens instrumentpanel (t.ex. GPS-navigationshistorik, webbsökningar osv.) rekommenderar Europeiska dataskyddsstyrelsen dessutom tillverkarna att tillhandahålla en enkel funktion (t.ex. en raderingsknapp).

92. Försäljning av ett uppkopplat fordon och påföljande ägarbyte bör också medföra radering av personuppgifter som inte längre behövs för de tidigare angivna ändamålen och den registrerade bör kunna utöva sin rätt till portabilitet.

2.7 Säkerhet

93. Tillverkare av fordon och utrustning, tjänsteleverantörer och andra personuppgiftsansvariga bör införa åtgärder som garanterar säkerheten och konfidentialiteten för behandlade uppgifter och vidta alla lämpliga försiktighetsåtgärder för att förhindra att en obehörig person tar över kontrollen. Branschaktörer bör särskilt överväga att vidta följande åtgärder:

- Kryptera kommunikationskanalerna med hjälp av en modern algoritm.
- Införa ett system för hantering av krypteringsnycklar som är unikt för varje fordon, inte för varje modell.
- Kryptera uppgifter med hjälp av moderna algoritmer vid lagring på distans.
- Regelbundet förnya krypteringsnycklarna.
- Skydda krypteringsnycklarna från utlämning.

- Autentisera anordningar som mottar uppgifter.
- Säkerställa dataintegritet (t.ex. genom hashning).
- Göra åtkomsten till personuppgifter beroende av tillförlitliga metoder för användarautentisering (lösenord, elektroniskt certifikat osv.).

94. När det mer specifikt gäller fordonstillverkare rekommenderar Europeiska dataskyddsstyrelsen att följande säkerhetsåtgärder genomförs:

- Skilja fordonets vitala funktioner från dem som alltid är beroende av telekommunikationskapacitet (t.ex. ”infotainment”).
- Genomföra tekniska åtgärder som gör det möjligt för fordonstillverkare att snabbt minska sårbarheter på säkerhetsområdet under fordonets hela livslängd.
- När det gäller fordonets vitala funktioner, i största möjliga utsträckning prioritera användningen av säkra kommunikationsmedel som är särskilt avsedda för transport.
- Inrätta ett larmsystem i händelse av angrepp på fordonets system, som eventuellt kan fungera vid nedsatt funktionsnivå[47].
- Spara en logghistorik över all åtkomst till fordonets informationssystem, t.ex. från de senaste sex månaderna som mest, för att göra det möjligt att förstå ursprunget till ett eventuellt angrepp och regelbundet granska den loggade informationen för att upptäcka eventuella anomalier.

95. Dessa allmänna rekommendationer bör kompletteras med särskilda krav som tar hänsyn till varje uppgiftsbehandlings särdrag och syfte.

2.8 Överföring av personuppgifter till tredje part

96. I princip är det endast den personuppgiftsansvarige och den registrerade som har tillgång till de uppgifter som genereras av ett uppkopplat fordon. Den personuppgiftsansvarige får dock överföra personuppgifter till en affärspartner (mottagare), i den mån en sådan överföring lagligen grundar sig på någon av de rättsliga grunder som anges i artikel 6 i dataskyddsförordningen.

97. Med tanke på känsligheten hos uppgifterna om fordonsanvändning (t.ex. genomförda resor, körstil) rekommenderar Europeiska dataskyddsstyrelsen att den registrerades samtycke systematiskt inhämtas innan hans eller hennes uppgifter överförs till en affärspartner som fungerar som personuppgiftsansvarig (t.ex. genom att kryssa i en ruta som inte är förkryssad eller, om det är tekniskt möjligt, genom att använda en fysisk eller logisk anordning som personen kan komma åt från fordonet). Affärspartnern blir i sin tur ansvarig för de uppgifter som den tar emot och omfattas av alla bestämmelser i dataskyddsförordningen.

98. Fordonstillverkaren, tjänsteleverantören eller annan personuppgiftsansvarig kan överföra personuppgifter till ett personuppgiftsbiträde som valts ut för att delta i tillhandahållandet av tjänsten till den registrerade, förutsatt att personuppgiftsbiträdet inte använder dessa

[47] Nedsatt funktionsnivå är ett driftläge för fordon som säkerställer att de funktioner som är väsentliga för säker drift av fordonet (dvs. minimikrav på säkerhet) garanteras även om andra mindre viktiga funktioner avaktiveras (t.ex. kan driften av navigationsutrustningen betraktas som icke väsentlig i motsats till bromssystemet).

uppgifter för eget bruk. Personuppgiftsansvariga och personuppgiftsbiträden ska upprätta ett avtal eller annat rättsligt dokument som specificerar varje parts skyldigheter och fastställer bestämmelserna enligt artikel 28 i dataskyddsförordningen.

2.9 Överföring av personuppgifter utanför EU/EES

99. Om personuppgifter överförs utanför Europeiska ekonomiska samarbetsområdet finns det särskilda skyddsåtgärder som säkerställer att skyddet följer med uppgifterna.

100. Som en följd av detta får den personuppgiftsansvarige överföra personuppgifter till en mottagare endast i den utsträckning som en sådan överföring är förenlig med kraven i kapitel V i dataskyddsförordningen.

2.10 Användning av wifi-teknik i fordon

101. Framsteg inom mobilteknik har gjort det möjligt att enkelt använda internet på vägarna. Även om det är möjligt att få wifi-uppkoppling i ett fordon via en surfpunkt från smarttelefonen eller en särskild anordning (OBD-II-dongel, trådlöst modem eller router osv.) erbjuder de flesta tillverkare nuförtiden modeller som har en inbyggd mobilanslutning och också kan skapa wifi-nätverk. Beroende på det enskilda fallet måste olika aspekter beaktas:

- Wifi-uppkopplingen erbjuds som en tjänst av trafikanställda, t.ex. av en taxichaufför till sina kunder. I detta fall kan yrkesutövaren eller dennes företag betraktas som en internetleverantör och därmed omfattas av särskilda skyldigheter och begränsningar när det gäller behandlingen av kundernas personuppgifter.

- Wifi-uppkopplingen är endast avsedd för föraren (uteslutande för användning av föraren och hans eller hennes passagerare). I detta fall anses behandling av personuppgifter vara verksamhet av rent privat natur eller hushållsverksamhet i enlighet med artikel 2.2 c och skäl 18 i dataskyddsförordningen.

102. I allmänhet innebär spridningen av gränssnitt för internetanslutning via wifi större risker för enskilda personers privatliv. Genom sina fordon skickar användarna nämligen kontinuerligt ut information och kan därmed identifieras och spåras. För att förhindra spårning bör tillverkarna av fordon och utrustning införa alternativ för opt-out som är lätta att använda och som säkerställer att SSID-namnet (*service set identifier*) på fordonets wifi-nätverk inte samlas in.

3 FALLSTUDIER

103. I detta avsnitt behandlas fem specifika exempel på behandling i samband med uppkopplade fordon, som motsvarar scenarier som sannolikt kan uppstå för berörda parter i sektorn. Exemplen omfattar behandling av uppgifter som kräver beräkning av effekt som inte kan mobiliseras lokalt i fordonet och/eller överföring av personuppgifter till en tredje part för att utföra ytterligare analys eller för att tillhandahålla ytterligare funktioner på distans. För varje typ av behandling anges i detta dokument de avsedda ändamålen, kategorierna av insamlade uppgifter, lagringstiden för sådana uppgifter, de registrerades rättigheter, de säkerhetsåtgärder som ska genomföras och mottagarna av informationen. Om några av dessa områden inte beskrivs nedan gäller de allmänna rekommendationer som beskrivs i föregående del.

104. De valda exemplen är inte uttömmande och är avsedda att visa på de många olika typer av behandling, rättsliga grunder, aktörer osv. som kan vara involverade inom ramen för uppkopplade fordon.

3.1 Tillhandahållande av en tjänst av en tredje part

105. Registrerade får ingå avtal med en tjänsteleverantör för att erhålla mervärdestjänster som rör deras fordon. En registrerad kan till exempel ingå ett användarbaserat försäkringsavtal som erbjuder lägre försäkringspremier för mindre körning (”Pay As You Drive”) eller bra körbeteende (”Pay How You Drive”) och som kräver att försäkringsbolaget övervakar körvanorna. En registrerad kan också ingå avtal med ett företag som erbjuder vägassistans i händelse av haveri och som innebär överföring av fordonets position till företaget eller med

en tjänsteleverantör för att ta emot meddelanden eller varningar om fordonets funktion (t.ex. en varning om bromsslitage eller en påminnelse om datum för besiktning).

3.1.1 Användarbaserad försäkring

106. ”Pay as you drive” är en typ av användarbaserad försäkring som följer förarens körsträcka och/eller körvanor för att differentiera och belöna ”säkra” förare genom att ge dem lägre premier. Försäkringsgivaren kommer att kräva att föraren installerar en inbyggd telematiktjänst eller en mobilapplikation eller aktiverar en inbyggd modul från tillverkningen som följer den sträcka som körs och/eller försäkringstagarens körbeteende (bromsmönster, snabb acceleration osv.). Den information som samlas in med hjälp av telematikutrustningen kommer att användas för att tilldela föraren poäng för att analysera vilka risker han eller hon kan innebära för försäkringsbolaget.

107. Eftersom användarbaserad försäkring kräver samtycke enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation anger Europeiska dataskyddsstyrelsen att försäkringstagaren måste kunna välja att teckna en icke-användningsbaserad försäkring. Annars skulle samtycket inte anses vara frivilligt, eftersom fullgörandet av avtalet skulle vara beroende av samtycket. Enligt artikel 7.3 i dataskyddsförordningen ska den registrerade dessutom ha rätt att återkalla sitt samtycke.

3.1.1.1 Rättslig grund

108. När uppgifterna samlas in genom en allmänt tillgänglig elektronisk kommunikationstjänst (t.ex. via SIM-kortet i telematikutrustningen) krävs samtycke för att få tillgång till information som redan lagras i fordonet i enlighet med artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Inget av de undantag som föreskrivs i dessa bestämmelser kan tillämpas i detta sammanhang: Behandlingen syftar inte enbart till att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät och avser inte heller en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt. Samtycke kan inhämtas vid tidpunkten för avtalets ingående.

109. När det gäller behandling av personuppgifter efter lagring eller tillgång till slutanvändarens terminalutrustning kan försäkringsbolaget i detta specifika sammanhang åberopa artikel 6.1 b i dataskyddsförordningen, förutsatt att det kan fastställa både att behandlingen äger rum inom ramen för ett giltigt avtal med den registrerade och att behandlingen är nödvändig för att det särskilda avtalet med den registrerade ska kunna fullgöras. I den mån behandlingen objektivt sett är nödvändig för fullgörandet av avtalet med den registrerade anser Europeiska dataskyddsstyrelsen att en tillämpning av artikel 6.1 b i dataskyddsförordningen inte skulle leda till att det ytterligare skydd som föreskrivs i artikel 5.3 i direktivet om integritet och elektronisk kommunikation minskas i detta specifika fall. Den rättsliga grunden förverkligas genom att den registrerade undertecknar ett avtal med försäkringsbolaget.

3.1.1.2 Insamlade uppgifter

110. Det finns två typer av personuppgifter som ska beaktas:

- **Kommersiella uppgifter och transaktionsuppgifter**: den registrerades identifieringsuppgifter, transaktionsrelaterade uppgifter, uppgifter om betalningsmedel osv.

- **Användningsuppgifter**: personuppgifter som genereras av fordonet, körvanor, plats osv.

111. Europeiska dataskyddsstyrelsen rekommenderar att rådata om körbeteende i möjligaste mån, och med tanke på att det finns en risk för att de uppgifter som samlas in via telematikboxen kan missbrukas för att skapa en exakt profil av förarens rörelser, antingen behandlas

- inuti fordonet i telematikboxar eller i användarens smarttelefon så att försäkringsgivaren endast får tillgång till resultatdata (t.ex. en poäng avseende körvanor), inte detaljerade rådata (se avsnitt 2.1),

- eller av leverantören av telematiktjänster för den personuppgiftsansvariges (försäkringsbolagets) räkning för att ge numeriska poäng som överförs till försäkringsbolaget på fastställd basis. I detta fall ska rådata och uppgifter som direkt rör förarens identitet separeras. Detta innebär att leverantören av telematiktjänster får realtidsdata, men inte känner till försäkringstagarnas namn, registreringsskyltar osv. Försäkringsgivaren känner däremot till försäkringstagarnas namn, men får endast poängen och det totala antalet kilometer och inte de rådata som används för att producera sådana poäng.

112. Det måste även noteras att lokaliseringsuppgifter inte ska samlas in om endast körsträckan krävs för fullgörandet av avtalet.

3.1.1.3 Lagringstid

113. I samband med uppgiftsbehandling som äger rum för fullgörandet av ett avtal (dvs. tillhandahållande av en tjänst) är det viktigt att skilja mellan två typer av uppgifter innan deras respektive lagringstid fastställs:

- **Kommersiella uppgifter och transaktionsuppgifter:** Dessa uppgifter kan lagras i en aktiv databas under hela avtalets löptid. När avtalet löper ut kan de arkiveras fysiskt (på ett separat medium: dvd osv.) eller logiskt (genom tillståndsförvaltning) i händelse av en eventuell rättstvist. Därefter ska uppgifterna raderas eller anonymiseras vid utgången av de lagstadgade preskriptionstiderna.

- **Användningsuppgifter:** Användningsuppgifter kan klassificeras som rådata och aggregerade uppgifter. Såsom anges ovan bör den personuppgiftsansvarige eller personuppgiftsbiträdet om möjligt inte behandla rådata. Om det är nödvändigt bör rådata bevaras endast så länge de är nödvändiga för att ta fram de aggregerade uppgifterna och kontrollera att denna aggregeringsprocess är giltig. Aggregerade uppgifter bör bevaras endast så länge som det är nödvändigt för tillhandahållandet av tjänsten eller när så krävs av andra skäl enligt unionsrätten eller medlemsstaternas lagstiftning.

3.1.1.4 Information till och rättigheter för registrerade

114. Före behandlingen av personuppgifter ska den registrerade informeras i enlighet med artikel 13 i dataskyddsförordningen på ett öppet och begripligt sätt. I synnerhet ska den registrerade informeras om den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period. I det sistnämnda fallet rekommenderar Europeiska dataskyddsstyrelsen att man tillämpar ett pedagogiskt tillvägagångssätt för att betona skillnaden mellan rådata och den poäng som tas fram på denna grund och betonar, när så är fallet, att försäkringsgivaren endast kommer att samla in resultatet av poängen när så är lämpligt.

115. Om uppgifter inte behandlas inuti fordonet utan av en telematikleverantör för den personuppgiftsansvariges (försäkringsbolagets) räkning kan det vara lämpligt att i

informationen nämna att leverantören i detta fall inte kommer att ha tillgång till uppgifter som direkt rör förarens identitet (t.ex. namn, registreringsskyltar osv.). Med tanke på vikten av att informera registrerade om konsekvenserna av behandlingen av deras personuppgifter och det faktum att registrerade inte bör överraskas av behandlingen av deras personuppgifter rekommenderar Europeiska dataskyddsstyrelsen att den registrerade informeras om förekomsten av profilering och konsekvenserna av sådan profilering, även om den inte inbegriper sådant automatiserat beslutsfattande som avses i artikel 22 i dataskyddsförordningen.

116. När det gäller registrerades rättigheter ska de särskilt informeras om vilka möjligheter de har att utöva sin rätt till åtkomst, rättelse, begränsning och radering. Eftersom rådata som samlas in i detta sammanhang tillhandahålls av den registrerade (genom särskilda formulär eller genom hans eller hennes aktivitet) och behandlas på grundval av artikel 6.1 b i dataskyddsförordningen (fullgörande av ett avtal) har den registrerade rätt att utöva sin rätt till dataportabilitet. Såsom betonas i riktlinjerna om rätten till dataportabilitet rekommenderar Europeiska dataskyddsstyrelsen starkt att ”personuppgiftsansvariga tydligt förklarar skillnaderna mellan de typer av uppgifter som en registrerad kan få ut via rätten till tillgång och rätten till dataportabilitet”[48].

117. Informationen kan lämnas när avtalet undertecknas.

3.1.1.5 Mottagare

118. Europeiska dataskyddsstyrelsen rekommenderar att fordonets användningsdata så långt det är möjligt behandlas direkt i telematikboxar, så att försäkringsgivaren endast får tillgång till resultatdata (t.ex. en poäng) och inte detaljerade rådata.

119. Om en leverantör av telematiktjänster samlar in uppgifterna för den personuppgiftsansvariges (försäkringsbolagets) räkning för att ge numeriska poäng behöver leverantören inte känna till förarens/försäkringstagarens identitet (t.ex. namn, registreringsskyltar osv.).

3.1.1.6 Säkerhet

120. Allmänna rekommendationer gäller. Se avsnitt 2.7.

3.1.2 Hyrning och bokning av parkeringsplats

121. Ägaren av en parkeringsplats kan vilja hyra ut den. För detta ändamål lägger han eller hon ut parkeringsplatsen och sätter ett pris på den i en webbapplikation. När parkeringsplatsen har lagts ut underrättar applikationen ägaren när en förare vill boka den. Föraren kan välja destination och söka efter tillgängliga parkeringsplatser utifrån flera kriterier. Efter ägarens godkännande bekräftas transaktionen och tjänsteleverantören hanterar betalningstransaktionen och använder sedan navigering för att köra till platsen.

3.1.2.1 Rättslig grund

122. När uppgifterna samlas in genom en allmänt tillgänglig elektronisk kommunikationstjänst gäller artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

123. Eftersom det rör sig om en av informationssamhällets tjänster krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation inte samtycke för att få tillgång till

[48] Artikel 29-arbetsgruppen, *Riktlinjer om rätten till dataportabilitet enligt förordning 2016/676*, WP242 rev. 01, godkända av Europeiska dataskyddsstyrelsen, s. 13.

information som redan finns lagrad i fordonet när abonnenten uttryckligen begär en sådan tjänst.

124. För behandling av personuppgifter och endast för uppgifter som är nödvändiga för fullgörandet av det avtal som den registrerade är part i kommer artikel 6.1 b i dataskyddsförordningen att vara den rättsliga grunden.

3.1.2.2 Insamlade uppgifter

125. De behandlade uppgifterna inkluderar förarens kontaktuppgifter (namn, e-postadress, telefonnummer, fordonstyp (t.ex. bil, lastbil, motorcykel)), registreringsnummer, parkeringsperiod, betalningsuppgifter (t.ex. kreditkortsuppgifter) samt navigationsdata.

3.1.2.3 Lagringstid

126. Uppgifter bör bevaras endast så länge som det är nödvändigt för att fullgöra parkeringsavtalet eller av andra skäl enligt unionsrätten eller medlemsstaternas lagstiftning. Efter det anonymiseras eller raderas uppgifterna.

3.1.2.4 Information till och rättigheter för registrerade

127. Före behandlingen av personuppgifter ska den registrerade informeras i enlighet med artikel 13 i dataskyddsförordningen på ett öppet och begripligt sätt.

128. Den registrerade ska särskilt informeras om vilka möjligheter han eller hon har att utöva sin rätt till åtkomst, rättelse, begränsning och radering. Eftersom uppgifter som samlas in i detta sammanhang tillhandahålls av den registrerade (genom särskilda formulär eller genom hans eller hennes aktivitet) och behandlas på grundval av artikel 6.1 b i dataskyddsförordningen (fullgörande av ett avtal) har den registrerade rätt att utöva sin rätt till dataportabilitet. Såsom betonas i riktlinjerna om rätten till dataportabilitet rekommenderar Europeiska dataskyddsstyrelsen starkt att ”personuppgiftsansvariga tydligt förklarar skillnaderna mellan de typer av uppgifter som en registrerad kan få ut via rätten till tillgång och rätten till dataportabilitet”.

3.1.2.5 Mottagare

129. I princip är det endast den personuppgiftsansvarige och personuppgiftsbiträdet som har tillgång till uppgifterna.

3.1.2.6 Säkerhet

130. Allmänna rekommendationer gäller. Se avsnitt 2.7.

3.2 eCall

131. Vid en allvarlig olycka i Europeiska unionen aktiverar fordonet automatiskt eCall till 112, det EU-omfattande larmnumret (se avsnitt 1.1 för närmare uppgifter), vilket gör det möjligt att snabbt skicka ambulans till olycksplatsen i enlighet med förordning (EU) 2015/758 av den 29 april 2015 om typgodkännandekrav för montering av eCall-system som bygger på 112-tjänsten i fordon och om ändring av direktiv 2007/46/EG (*förordning (EU) 2015/758*).

132. Den eCall-generator som installerats i fordonet, som möjliggör överföring via ett allmänt trådlöst mobilkommunikationsnät, initierar ett nödsamtal som antingen aktiveras automatiskt genom fordonssensorer eller manuellt av de personer som befinner sig i fordonet, endast i händelse av en olycka. Förutom aktivering av ljudkanalen består den andra händelsen som aktiveras automatiskt vid en olycka i att en minimiuppsättning uppgifter (MSD) genereras och skickas till larmcentralen.

3.2.1 Rättslig grund

133. När det gäller tillämpningen av direktivet om integritet och elektronisk kommunikation måste två bestämmelser beaktas:

- Artikel 9 om andra lokaliseringsuppgifter än trafikuppgifter, som endast gäller elektroniska kommunikationstjänster.
- Artikel 5.3 om tillgång till information som är lagrad i den generator som är installerad i fordonet.

134. Trots att dessa bestämmelser i princip kräver den registrerades samtycke utgör förordning (EU) 2015/758 en rättslig skyldighet som den personuppgiftsansvarige omfattas av (den registrerade har inget verkligt eller fritt val och kommer inte att kunna motsätta sig att hans eller hennes uppgifter behandlas). I förordning (EU) 2015/758 åsidosätts därför behovet av förarens samtycke för behandling av lokaliseringsuppgifter och MSD[49].

135. Den rättsliga grunden för behandlingen av dessa uppgifter kommer att vara efterlevnad av en rättslig skyldighet enligt artikel 6.1 c i dataskyddsförordningen (dvs. förordning (EU) 2015/758).

3.2.2 Insamlade uppgifter

136. I förordning (EU) 2015/758 föreskrivs att uppgifter som översänds av det 112-baserade eCall-systemet i fordon endast ska omfatta den minimiinformation som avses i standarden EN 15722:2015 *Intelligent transport systems – eSafety – eCall minimum set of data (MSD)*, som innefattar följande:

- Uppgift om huruvida eCall har aktiverats manuellt eller automatiskt.
- Fordonstyp.
- Fordonets identifieringsnummer (VIN).
- Fordonets framdrivningstyp.
- Tidsmarkering för den första genereringen av datameddelanden inom den aktuella eCall-incidenten.
- Senast kända position för fordonets latitud och longitud fastställd vid den senast möjliga tidpunkten före genereringen av meddelandet.
- Fordonets senaste kända verkliga färdriktning fastställd vid den senast möjliga tidpunkten före genereringen av meddelandet (endast fordonets tre sista positioner).

3.2.3 Lagringstid

137. I förordning (EU) 2015/758 föreskrivs att uppgifter inte ska bevaras längre än vad som är nödvändigt för att hantera nödsituationer. Dessa uppgifter ska raderas så snart de inte längre behövs för detta ändamål. Dessutom ska uppgifter i eCall-systemets internminne raderas automatiskt och kontinuerligt. Endast uppgifter om fordonets tre sista positioner

[49] Det bör noteras att artikel 8.1 f i rådets förhandlingsmandat för förslaget till förordning om integritet och elektronisk kommunikation innehåller ett särskilt undantag för eCall, eftersom samtycke inte behövs när det är nödvändigt att lokalisera terminalutrustning när en slutanvändare gör en nödkommunikation antingen till det gemensamma europeiska larmnumret 112 eller till ett nationellt larmnummer, i enlighet med artikel 13.3.

kan bevaras i den mån det är absolut nödvändigt för att fastställa fordonets aktuella position och färdriktning vid tidpunkten för händelsen.

3.2.4 Information till och rättigheter för registrerade

138. Enligt artikel 6 i förordning (EU) 2015/758 ska tillverkarna tillhandahålla tydlig och fullständig information om den behandling av uppgifter som görs i eCall-systemet. Denna information ska tillhandahållas separat i instruktionsboken för det 112-baserade eCall-systemet i fordon och eventuella eCall-system i tredje parts regi innan systemet används. Den omfattar följande:

- Hänvisning till behandlingens rättsliga grund.
- Att det 112-baserade eCall-systemet i fordon är aktiverat som standardinställning.
- Formerna för den behandling av uppgifter som det 112-baserade eCall-systemet i fordon utför.
- Det specifika syftet med eCall-behandlingen, vilket ska vara begränsat till de nödsituationer som avses i artikel 5.2 första stycket i förordning (EU) 2015/758.
- De typer av uppgifter som samlas in och behandlas och de uppgifternas mottagare.
- Tidsgränsen för lagring av uppgifter i det 112-baserade eCall-systemet i fordon.
- Det faktum att fordonet inte spåras kontinuerligt.
- Formerna för utövande av den registrerades rättigheter och den kontakttjänst som är behörig för hanteringen av ansökningar om tillgång.
- Alla nödvändiga ytterligare upplysningar om spårbarhet, spårning och behandling av personuppgifter inom en eCall-tjänst i tredje parts regi (*TPS-eCall-tjänst*) och/eller andra mervärdestjänster, vilka uttryckligen ska godkännas av användaren och vara förenliga med dataskyddsförordningen. Särskild hänsyn ska tas till att det kan finnas skillnader mellan den behandling av uppgifter som utförs genom det 112-baserade eCall-systemet i fordon och den behandling som utförs genom TPS-eCall-systemen i fordon eller andra mervärdestjänster.

139. Tjänsteleverantören ska dessutom tillhandahålla de registrerade information i enlighet med artikel 13 i dataskyddsförordningen på ett öppet och begripligt sätt. I synnerhet ska de informeras om ändamålen med den behandling för vilken personuppgifterna är avsedda samt om att behandlingen av personuppgifter grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

140. Dessutom bör informationen om mottagarna eller kategorierna av mottagare av personuppgifterna, med beaktande av behandlingens art, vara tydlig och de registrerade bör informeras om att uppgifterna inte är tillgängliga utanför det 112-baserade eCall-systemet i fordon för några andra enheter innan eCall aktiveras.

141. När det gäller de registrerades rättigheter måste det noteras att eftersom behandlingen grundar sig på en rättslig förpliktelse kommer rätten att göra invändningar och rätten till portabilitet inte att gälla.

3.2.5 Mottagare

142. Uppgifterna får inte finnas tillgängliga utanför det 112-baserade eCall-systemet i fordon för några enheter innan eCall-systemet aktiveras.

143. När eCall-systemet aktiveras (antingen manuellt av personer som befinner sig i fordonet eller automatiskt så snart en sensor i fordonet upptäcker en allvarlig kollision) upprättar det en röstanslutning till den relevanta larmcentralen och MSD skickas till larmcentralens operatör.

144. De uppgifter som överförs via det 112-baserade eCall-systemet i fordon och behandlas av larmcentralerna kan endast överföras till den larmtjänst och till de servicepartner som avses i beslut nr 585/2014/EU vid olyckor med anknytning till eCall och enligt de villkor som fastställs i det beslutet, och de används enbart för att uppnå målen i det beslutet. Uppgifter som behandlas av larmtjänster via det 112-baserade eCall-systemet i fordon överförs inte till några andra tredjeparter utan uttryckligt förhandsgodkännande från den registrerade.

3.2.6 Säkerhet

145. I förordning (EU) 2015/758 fastställs kraven på att i eCall-systemet bygga in teknik som stärker integritetsskyddet för att ge användarna lämpligt integritetsskydd och de garantier som behövs för att förhindra övervakning och missbruk. Tillverkarna bör dessutom se till att det 112-baserade eCall-systemet, liksom alla andra system som erbjuder eCall i tredje parts regi eller en mervärdestjänst, är utformade så att det är omöjligt att utbyta personuppgifter mellan dessa system.

146. När det gäller larmcentraler ska medlemsstaterna säkerställa att personuppgifter skyddas mot missbruk, inklusive olaglig åtkomst, ändring eller förlust, och att de protokoll som avser lagring av personuppgifter, bibehållande, behandling och skydd upprättas på lämplig nivå och iakttas.

3.3 Olycksundersökningar

147. Registrerade kan frivilligt gå med på att delta i olycksundersökningar som syftar till att skapa större förståelse av orsakerna till trafikolyckor och mer allmänt till vetenskapliga ändamål.

3.3.1 Rättslig grund

148. När uppgifterna samlas in via en offentlig elektronisk kommunikationstjänst måste den personuppgiftsansvarige inhämta den registrerades samtycke för att få tillgång till information som redan är lagrad i fordonet i enlighet med artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Inget av de undantag som föreskrivs i dessa bestämmelser kan tillämpas i detta sammanhang: Behandlingen syftar inte enbart till att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät och avser inte heller en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.

149. När det gäller behandlingen av personuppgifter och med beaktande av de många olika personuppgifter som behövs för olycksundersökningar rekommenderar Europeiska dataskyddsstyrelsen att behandlingen baseras på den registrerades förhandssamtycke i enlighet med artikel 6 i dataskyddsförordningen. Ett sådant förhandssamtycke måste lämnas på en särskild blankett genom vilken den registrerade frivilligt går med på att delta i undersökningen och låta sina personuppgifter behandlas för detta ändamål. Samtycket ska vara ett uttryck för den fria, specifika och informerade viljan hos den person vars uppgifter behandlas (t.ex. genom att kryssa i en ruta som inte är förkryssad eller konfigurera fordonsdatorn för att aktivera en funktion i fordonet). Sådant samtycke ska tillhandahållas separat, för särskilda ändamål, får inte inbakas i ett avtal för att köpa eller leasa en ny bil, och samtycket ska kunna återkallas lika lätt som det har getts. Återkallande av samtycke ska

leda till att behandlingen stoppas. Uppgifterna ska sedan raderas från den aktiva databasen eller anonymiseras.

150. Samtycke som krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation och samtycke som krävs som rättslig grund för behandling av uppgifter kan hämtas samtidigt (t.ex. genom att kryssa i en ruta som tydligt anger vad den registrerade samtycker till).

151. Det bör noteras att beroende på villkoren för behandlingen (typen av personuppgiftsansvarig osv.) kan en annan rättslig grund lagligen väljas så länge den inte minskar det ytterligare skydd som föreskrivs i artikel 5.3 i direktivet om integritet och elektronisk kommunikation (se punkt 15). Om behandlingen grundar sig på en annan rättslig grund, såsom utförandet av en uppgift av allmänt intresse (artikel 6.1 e i dataskyddsförordningen), rekommenderar Europeiska dataskyddsstyrelsen att de registrerade inkluderas i undersökningen på frivillig basis.

3.3.2 Insamlade uppgifter

152. Den personuppgiftsansvarige ska endast samla in personuppgifter som är absolut nödvändiga för behandlingen.

153. Det finns två typer av uppgifter som ska beaktas:

- **Uppgifter om deltagare och fordon**.
- **Tekniska uppgifter från fordon** (momentan hastighet osv.).

154. Vetenskaplig olycksfallsforskning motiverar insamlingen av den momentana hastigheten, även av juridiska personer som inte administrerar en offentlig tjänst i egentlig mening.

155. Som konstaterats ovan anser Europeiska dataskyddsstyrelsen att uppgifter om momentan hastighet som samlas in i samband med en olycksundersökning inte per definition är brottsrelaterade uppgifter (dvs. de samlas inte in för att utreda eller lagföra ett brott), vilket motiverar att de samlas in av juridiska personer som inte administrerar en offentlig tjänst i egentlig mening.

3.3.3 Lagringstid

156. Det är viktigt att skilja mellan två typer av uppgifter. För det första kan uppgifter om deltagare och fordon bevaras tills undersökningen är slutförd. För det andra bör de tekniska uppgifterna från fordon bevaras så kort som möjligt för ändamålet. I detta avseende förefaller fem år från undersökningens slutdatum vara en rimlig tidsperiod. Vid utgången av denna period ska uppgifterna raderas eller anonymiseras.

3.3.4 Information till och rättigheter för registrerade

157. Före behandlingen av personuppgifter ska den registrerade informeras i enlighet med artikel 13 i dataskyddsförordningen på ett öppet och begripligt sätt. I synnerhet när det gäller insamling av momentan hastighet bör de registrerade informeras särskilt om uppgiftsinsamlingen. Eftersom behandlingen av uppgifter grundar sig på samtycke måste den registrerade informeras särskilt om rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Eftersom uppgifter som samlas in i detta sammanhang dessutom tillhandahålls av den registrerade (genom särskilda formulär eller genom hans eller hennes aktivitet) och behandlas på grundval av artikel 6.1 a i dataskyddsförordningen (samtycke) har den

registrerade rätt att utöva sin rätt till dataportabilitet. Såsom betonas i riktlinjerna om rätten till dataportabilitet rekommenderar Europeiska dataskyddsstyrelsen starkt att ”personuppgiftsansvariga tydligt förklarar skillnaderna mellan de typer av uppgifter som en registrerad kan få ut via rätten till tillgång och rätten till dataportabilitet”. Följaktligen bör den personuppgiftsansvarige tillhandahålla ett enkelt sätt att återkalla samtycket, frivilligt och när som helst, samt utveckla verktyg för att kunna besvara begäranden om dataportabilitet.

158. Denna information kan lämnas vid undertecknandet av det formulär där samtycke ges till att delta i olycksundersökningen.

3.3.5 Mottagare

159. I princip är det endast den personuppgiftsansvarige och personuppgiftsbiträdet som har tillgång till uppgifterna.

3.3.6 Säkerhet

160. Såsom anges ovan ska de säkerhetsåtgärder som införs anpassas till uppgifternas känslighet. Om till exempel uppgifter om momentan hastighet (eller andra uppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott) samlas in som en del av olycksundersökningen rekommenderar Europeiska dataskyddsstyrelsen starkt att kraftfulla säkerhetsåtgärder införs, såsom

- genomförande av åtgärder för pseudonymisering (t.ex. hashning med en privat nyckel av uppgifter såsom den registrerades efternamn/förnamn och serienumret),
- lagring av uppgifter om momentan hastighet och plats i separata databaser (t.ex. med hjälp av en modern krypteringsmekanism med särskilda nycklar och godkännandemekanismer),
- och/eller radering av lokaliseringsuppgifter så snart referenshändelsen eller referenssekvensen är kvalificerad (t.ex. typ av väg, dag/natt) och lagring av uppgifter som direkt identifierar en person i en separat databas som endast kan nås av ett fåtal personer.

3.4 Bekämpning av bilstöld

161. Registrerade kan vid stöld vilja försöka hitta sitt fordon med hjälp av platsen. Användningen av lokaliseringsuppgifter är begränsad till det som är strikt nödvändigt för utredningen och till de behöriga rättsliga myndigheternas bedömning av ärendet.

3.4.1 Rättslig grund

162. När uppgifterna samlas in genom en allmänt tillgänglig elektronisk kommunikationstjänst gäller artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

163. Eftersom det rör sig om en av informationssamhällets tjänster krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation inte samtycke för att få tillgång till information som redan finns lagrad i fordonet när abonnenten uttryckligen begär en sådan tjänst.

164. När det gäller behandling av personuppgifter kommer den rättsliga grunden för behandling av lokaliseringsuppgifterna att vara fordonsägarens samtycke eller, i tillämpliga fall, fullgörande av ett avtal (endast för uppgifter som är nödvändiga för fullgörandet av det avtal som fordonsägaren är part i).

165. Samtycket ska vara ett uttryck för den fria, specifika och informerade viljan hos den person vars uppgifter behandlas (t.ex. genom att kryssa i en ruta som inte är förkryssad eller konfigurera fordonsdatorn för att aktivera en funktion i fordonet). Friheten att lämna samtycke innebär en möjlighet att när som helst återkalla samtycket, vilket den registrerade uttryckligen bör informeras om. Återkallande av samtycke ska leda till att behandlingen stoppas. Uppgifterna ska sedan raderas från den aktiva databasen, anonymiseras eller arkiveras.

3.4.2 Insamlade uppgifter

166. Lokaliseringsuppgifter kan endast överföras från och med stöldanmälan och kan inte samlas in kontinuerligt under resten av tiden.

3.4.3 Lagringstid

167. Lokaliseringsuppgifter får endast bevaras under den period då ärendet bedöms av de behöriga rättsliga myndigheterna eller fram till slutet av ett förfarande för att undanröja tvivel som inte avslutas med bekräftelse av att fordonet stulits.

3.4.4 Information till registrerade

168. Före behandlingen av personuppgifter ska den registrerade informeras i enlighet med artikel 13 i dataskyddsförordningen på ett öppet och begripligt sätt. Europeiska dataskyddsstyrelsen rekommenderar mer specifikt att den personuppgiftsansvarige betonar att fordonet inte spåras kontinuerligt och att lokaliseringsuppgifter endast kan samlas in och överföras från och med stöldanmälan. Dessutom måste den personuppgiftsansvarige ge den registrerade information om att endast godkända tjänstemän vid plattformen för fjärrövervakning och rättsligt godkända myndigheter har tillgång till uppgifterna.

169. När det gäller de registrerades rättigheter bör den registrerade, när behandlingen av uppgifter grundar sig på samtycke, informeras särskilt om rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. När uppgifter som samlas in i detta sammanhang tillhandahålls av den registrerade (genom särskilda formulär eller genom hans eller hennes aktivitet) och behandlas på grundval av artikel 6.1 a (samtycke) eller artikel 6.1 b i dataskyddsförordningen (fullgörande av ett avtal) har den registrerade dessutom rätt att utöva sin rätt till dataportabilitet. Såsom betonas i riktlinjerna om rätten till dataportabilitet rekommenderar Europeiska dataskyddsstyrelsen starkt att ”personuppgiftsansvariga tydligt förklarar skillnaderna mellan de typer av uppgifter som en registrerad kan få ut via rätten till tillgång och rätten till dataportabilitet”.

170. Följaktligen bör den personuppgiftsansvarige tillhandahålla ett enkelt sätt att återkalla samtycket (endast när samtycke är den rättsliga grunden), frivilligt och när som helst, samt utveckla verktyg för att kunna besvara begäranden om dataportabilitet.

171. Informationen kan lämnas när avtalet undertecknas.

3.4.5 Mottagare

172. Vid stöldanmälan kan lokaliseringsuppgifter överföras till i) godkända tjänstemän på plattformen för fjärrövervakning och ii) till de lagligen godkända myndigheterna.

3.4.6 Säkerhet

173. Allmänna rekommendationer gäller. Se avsnitt 2.7.