Ohjeet 1/2020 henkilötietojen käsittelystä verkkoon liitettyjen ajoneuvojen ja liikkuvuuteen liittyvien sovellusten yhteydessä

Versio 2.0

Annettu 9. maaliskuuta 2021

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

Versioyhteenveto

Versio 2.0	9. maaliskuuta 2021	Ohjeiden hyväksyminen julkisen kuulemisen jälkeen
Versio 1.0	28. tammikuuta 2020	Ohjeiden hyväksyminen julkista kuulemista varten

Sisällysluettelo

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus' tai 'asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETAn sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON HYVÄKSYNYT SEURAAVAT OHJEET:

1 JOHDANTO

1. Auto on 1900-luvun talouden symboli, ja se on yksi niistä massakulutushyödykkeistä, jotka ovat vaikuttaneet koko yhteiskuntaan. Autoihin liittyy yleisesti vapauden käsite, ja ne ovat usein muutakin kuin pelkkiä kuljetusvälineitä. Ne edustavat yksityisaluetta, jolla ihmiset voivat tehdä itsenäisiä päätöksiä ilman ulkoisia häiriöitä. Tämä visio ei enää vastaa todellisuutta, kun verkkoon liitetyistä ajoneuvoista tulee yhä yleisempiä. Ajoneuvojen sisäiset yhteydet ovat nopeasti siirtymässä luksusmalleista ja huippumerkeistä massatuotettuihin keskihintaisiin malleihin, ja ajoneuvoista on tulossa valtavia tietokeskuksia. Ajoneuvojen lisäksi myös kuljettajat ja matkustajat ovat yhä enemmän yhteydessä verkkoon. Itse asiassa monet markkinoille viime vuosina tuodut mallit sisältävät antureita ja verkkoon liitettyjä ajoneuvolaitteita, jotka voivat kerätä ja tallentaa tietoa muun muassa moottorin suorituskyvystä, ajotottumuksista, käyntikohteista ja mahdollisesti jopa kuljettajan silmänliikkeistä ja pulssista tai biometrisiä tietoja luonnollisen henkilön yksiselitteistä tunnistamista varten.[2]

2. Tällainen tietojenkäsittely tapahtuu monimutkaisessa ekosysteemissä, jolle on ilmaantunut autoteollisuuden perinteisten toimijoiden lisäksi myös uusia digitaalitalouden toimijoita. Nämä uudet toimijat voivat tarjota viihde- ja tietopalveluja, kuten musiikkia tai tietoa teiden kunnosta ja liikenteestä, tai tarjota kuljettajan apujärjestelmiä ja palveluja, kuten automaattiohjausohjelmistoja, ilmoituksia ajoneuvon kunnosta, käyttöön perustuvia vakuutuksia tai dynaamisia karttoja. Koska ajoneuvot on liitetty verkkoon sähköisten viestintäverkkojen välityksellä, myös tähän prosessiin osallistuvilla tieinfrastruktuurin haltijoilla ja teleoperaattoreilla on tärkeä rooli kuljettajien ja matkustajien henkilötietojen mahdollisissa käsittelytoimissa.

3. Lisäksi verkkoon liitetyt ajoneuvot tuottavat yhä enemmän tietoa, josta suurin osa voidaan katsoa henkilötiedoiksi, koska ne liittyvät kuljettajiin tai matkustajiin. Vaikka verkkoon liitetyn auton keräämät tiedot eivät liity suoraan tiettyyn nimeen vaan ajoneuvon teknisiin

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETAn jäsenvaltioita.
[2] Yksityisyyden suojaa käsittelevän Future of Privacy Forumin infografiikka "Data and the connected car"; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

näkökohtiin ja ominaisuuksiin, ne koskevat auton kuljettajaa tai matkustajia. Esimerkkinä voidaan mainita, että ajotyyliin tai ajettuun matkaan liittyvät tiedot, ajoneuvon osien kulumista koskevat tiedot, sijaintitiedot tai kameroiden keräämät tiedot voivat koskea kuljettajan käyttäytymistä sekä myös muita mahdollisesti ajoneuvon sisällä olevia henkilöitä tai ohi kulkevia rekisteröityjä. Tällaiset tekniset tiedot tuottaa luonnollinen henkilö, ja niiden perusteella rekisterinpitäjä tai muu henkilö voi tunnistaa hänet suoraan tai välillisesti. Ajoneuvoa voidaan pitää päätelaitteena, jota eri käyttäjät voivat käyttää. Kuten henkilökohtaisten tietokoneiden tapauksessa, se, että käyttäjiä voi olla useita, ei vaikuta siihen, että tiedot ovat luonteeltaan henkilötietoja.

4. Vuonna 2016 Kansainvälinen autoliitto Fédération Internationale de l'Automobile (FIA) järjesti "My Car My Data" -kampanjan[3] koko Euroopassa saadakseen käsityksen siitä, miten eurooppalaiset suhtautuvat verkkoon liitettyihin autoihin. Vaikka kampanja osoitti, että kuljettajat ovat erittäin kiinnostuneita liitettävyydestä, siitä kävi myös ilmi, että ajoneuvojen tuottamien tietojen käytössä tarvitaan valppautta ja että henkilötietojen suojaa koskevaa lainsäädäntöä on tärkeää noudattaa. Näin ollen kunkin sidosryhmän haasteena on ottaa henkilötietojen suoja huomioon tuotteen suunnitteluvaiheesta alkaen ja varmistaa, että autojen käyttäjien tietojen käsittely on läpinäkyvää ja että käyttäjät voivat valvoa tietojaan yleisen tietosuoja-asetuksen johdanto-osan 78 kappaleen mukaisesti. Tällainen lähestymistapa auttaa vahvistamaan käyttäjien luottamusta ja siten kehittämään kyseisiä teknologioita pitkällä aikavälillä.

1.1 Muut julkaisut

5. Verkkoon liitetyistä ajoneuvoista on tullut viimeisten kymmenen vuoden aikana sääntelyviranomaisten kannalta merkittävä aihe, ja tällaisten ajoneuvojen määrä on kasvanut huomattavasti parin viime vuoden aikana. Tästä syystä kansallisella ja kansainvälisellä tasolla on laadittu erilaisia verkkoon liitettyjen ajoneuvojen turvallisuutta ja yksityisyyttä koskevia julkaisuja. Kyseisillä säädöksillä ja aloitteilla pyritään täydentämään nykyisiä tietosuojaa ja yksityisyyden suojaa koskevaa kehystä alakohtaisilla säännöillä tai antamaan ohjeita ammattilaisille.

1.1.1 Euroopan tason aloitteet ja kansainväliset aloitteet

6. Hätänumeroon 112 perustuva ajoneuvoon asennettava eCall-järjestelmä on ollut pakollinen 31. maaliskuuta 2018 alkaen kaikissa uusissa M1- ja N1-luokan ajoneuvotyypeissä (henkilöautot ja kevyet hyötyajoneuvot).[4][5] Tietosuojatyöryhmä oli jo hyväksynyt vuonna 2006 valmisteluasiakirjan eCall-aloitteen vaikutuksista tietosuojaan ja yksityisyyteen[6]. Lisäksi tietosuojatyöryhmä antoi aiemman keskustelun mukaisesti lokakuussa 2017 lausunnon henkilötietojen käsittelystä vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) yhteydessä.

---

[3] "My Car My Data" -kampanja; http://www.mycarmydata.eu/

[4] Yhteentoimiva EU:n laajuinen hätäpuhelujärjestelmä (eCall); https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

[5] Euroopan parlamentin ja neuvoston päätös N:o 585/2014/EU, annettu 15 päivänä toukokuuta 2014, yhteentoimivan EU:n laajuisen eCall-palvelun käyttöönotosta (ETA:n kannalta merkityksellinen teksti); https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32014D0585

[6] Valmisteluasiakirja eCall-aloitteen vaikutuksista tietosuojaan ja yksityisyyteen; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_fi.pdf

7. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) julkaisi tammikuussa 2017 tutkimuksen[7], jossa tarkastellaan älykkäiden autojen kyberturvallisuutta ja häiriönsietokykyä. Tutkimuksessa luetellaan herkät ominaisuudet sekä niihin liittyvät uhat, riskit, lieventävät tekijät ja mahdolliset toteutettavat turvatoimet. Syyskuussa 2017 tietosuojavaltuutettujen kansainvälinen konferenssi (ICDPPC) antoi päätöslauselman verkkoon liitetyistä ajoneuvoista[8]. Huhtikuussa 2018 myös telealan tietosuojakysymysten kansainvälinen työryhmä (International Working Group on Data Protection in Telecommunications, IWGDPT) antoi verkkoon liitettyjä ajoneuvoja koskevan valmisteluasiakirjan[9].

1.1.2 Euroopan tietosuojaneuvoston jäsenten kansalliset aloitteet

8. Saksan liittovaltion ja osavaltioiden tietosuojaviranomaisten konferenssi ja Saksan autoteollisuusliitto (VDA) julkaisivat tammikuussa 2016 yhteisen julistuksen verkkoon liitettyjen ja muiden kuin verkkoon liitettyjen ajoneuvojen tietosuojaperiaatteista[10]. Yhdistyneen kuningaskunnan verkkoon liitetyistä ja automaattisista ajoneuvoista vastaava keskus (CCAV) julkaisi elokuussa 2017 oppaan, jossa esitetään verkkoon liitettyjen ja automaattisten ajoneuvojen kyberturvallisuuden periaatteet[11]. Tarkoituksena oli lisätä tietoisuutta asiasta autoalalla. Ranskan tietosuojaviranomainen, Commission nationale de l'Informatique et des Libertés (CNIL), julkaisi lokakuussa 2017 verkkoon liitettyjä autoja koskevan vaatimustenmukaisuuspaketin[12] sidosryhmien avuksi sisäänrakennetun ja oletusarvoisen tietosuojan huomioon ottamisessa, jotta rekisteröidyt voivat valvoa tietojaan tehokkaasti.

1.2 Sovellettava lainsäädäntö

9. Asiaa koskeva EU:n oikeudellinen kehys on yleinen tietosuoja-asetus. Sitä sovelletaan kaikissa tapauksissa, joissa verkkoon liitettyihin ajoneuvoihin liittyvään tietojenkäsittelyyn sisältyy yksilöiden henkilötietojen käsittelyä.

10. Yleisen tietosuoja-asetuksen lisäksi direktiivissä 2002/58/EY, sellaisena kuin se on muutettuna direktiivillä 2009/136/EY, jäljempänä 'sähköisen viestinnän tietosuojadirektiivi', **vahvistetaan erityiset vaatimukset kaikille toimijoille, jotka haluavat tallentaa tai käyttää tilaajan tai käyttäjän päätelaitteelle tallennettuja tietoja Euroopan talousalueella (ETA)**.

11. Siinä missä suurinta osaa sähköisen viestinnän tietosuojadirektiivin säännöksistä (6 artikla, 9 artikla jne.) sovelletaan vain yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajiin ja yleisten viestintäverkkojen tarjoajiin, sähköisen viestinnän tietosuojadirektiivin

[7] Älykkäiden autojen kyberturvallisuus ja häiriönsietokyky; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[8] Päätöslauselma automatisoitujen ja verkkoon liitettyjen ajoneuvojen tietosuojasta; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

[9] Valmisteluasiakirja verkkoon liitetyistä ajoneuvoista; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/

[10] Verkkoon liitettyjen ja muiden kuin verkkoon liitettyjen ajoneuvojen käyttöön liittyvät tietosuojanäkökohdat; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf

[11] Verkkoon liitettyjen ja automaattisten ajoneuvojen kyberturvallisuuden periaatteet; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[12] Vaatimustenmukaisuuspaketti tietojen vastuullisesta käytöstä verkkoon liitetyissä autoissa; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

5 artiklan 3 kohta on yleinen säännös. Sitä sovelletaan sähköisten viestintäpalvelujen lisäksi kaikkiin yksityisiin tai julkisiin tahoihin, jotka tallentavat päätelaitteelle tai lukevat sieltä tietoja riippumatta tallennettavien tai käsiteltävien tietojen luonteesta.

12. ”*Päätelaitteen*” määritelmä annetaan direktiivissä 2008/63/EY[13]. Direktiivin 1 artiklan 1 kohdan a alakohdan mukaan päätelaitteella tarkoitetaan ”*suoraan tai välillisesti yleisen televerkon rajapintaan liitettyä tietojen lähettämiseen, käsittelyyn tai vastaanottamiseen tarkoitettua laitetta; molemmissa tapauksissa (suora tai välillinen) liitäntä voidaan tehdä johdoin, optisella kuidulla tai sähkömagneettisesti; yhteys on välillinen, jos on sijoitettu laite päätelaitteen ja verkon rajapinnan väliin; b) satelliittimaa-asemalaitteita”.*

13. Jos edellä mainitut kriteerit täyttyvät, verkkoon liitettyä ajoneuvoa ja siihen liitettyä laitetta olisi näin ollen pidettävä ”*päätelaitteina*” (kuten tietokonetta, älypuhelinta tai älytelevisiota), ja tarvittaessa sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan säännöksiä.

14. Kuten Euroopan tietosuojaneuvosto on todennut sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta antamassaan lausunnossa 5/2019[14], sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädetään, että yleensä tietojen tallentamiseen tai tilaajan tai käyttäjän päätelaitteelle tallennettujen tietojen käyttämiseen tarvitaan etukäteissuostumus, jollei jäljempänä alakohdassa 17 mainituista poikkeuksista muuta johdu. Siltä osin kuin loppukäyttäjien laitteelle tallennetut tiedot ovat henkilötietoja, sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohta on etusijalla yleisen tietosuoja-asetuksen 6 artiklaan nähden toiminnassa, jossa nämä tiedot tallennetaan tai niitä käytetään.[15] Jotta edellä mainittujen käsittelytoimien jälkeen suoritettava henkilötietojen käsittely, mukaan lukien päätelaitteessa olevien tietojen perusteella saatujen henkilötietojen käsittely, olisi lainmukaista, sillä on oltava yleisen tietosuoja-asetuksen 6 artiklan mukainen oikeusperuste.[16]

15. Kun rekisterinpitäjä hakee suostumusta tietojen tallentamiseen tai tietojen saantiin sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaisesti, rekisterinpitäjän on ilmoitettava rekisteröidylle käsittelyn kaikista tarkoituksista – mukaan lukien kaikki käsittely edellä mainittujen toimintojen jälkeen (eli jatkokäsittely) – yleisen tietosuoja-asetuksen 6 artiklan mukainen suostumus on yleensä asianmukaisin oikeusperuste tällaisten toimien jälkeistä henkilötietojen käsittelyä varten (siltä osin kuin myöhemmän käsittelyn tarkoitus sisältyy rekisteröidyn suostumukseen, ks. kohdat 53–54 jäljempänä). Näin ollen suostumus muodostaa todennäköisesti oikeusperusteen jo tallennettujen tietojen tallentamiselle ja niiden käyttämiselle sekä henkilötietojen jatkokäsittelylle.[17]

---

[13] Komission direktiivi 2008/63/EY, annettu 20 päivänä kesäkuuta 2008, kilpailusta telepäätelaitemarkkinoilla (kodifioitu toisinto) (ETA:n kannalta merkityksellinen teksti); https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A32008L0063

[14] Euroopan tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, annettu 12. maaliskuuta 2019, jäljempänä ’lausunto 5/2019’, alakohta 40.

[15] Sama kuin edellä, alakohta 40.

[16] Sama kuin edellä, alakohta 41.

[17] Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa edellytetty suostumus ja tietojen käsittelyn oikeusperusteeksi tarvittava suostumus (yleisen tietosuoja-asetuksen 6 artikla) samaa tarkoitusta varten voidaan kerätä samaan aikaan (esimerkiksi merkitään rasti ruutuun, josta käy selvästi ilmi, mihin rekisteröity antaa suostumuksensa).

Arvioitaessa yleisen tietosuoja-asetuksen 6 artiklan noudattamista olisikin otettava huomioon, että käsittelyyn liittyy kokonaisuutena erityistoimia, joiden osalta EU:n lainsäätäjä on pyrkinyt antamaan lisäsuojaa.[18] Rekisterinpitäjien on lisäksi otettava huomioon vaikutus rekisteröityjen oikeuksiin määrittäessään asianmukaista oikeusperustetta kohtuullisuuden periaatteen noudattamiseksi.[19] Lähtökohtana on, että rekisterinpitäjät eivät voi vedota yleisen tietosuoja-asetuksen 6 artiklaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädetyn lisäsuojan heikentämiseksi.

16. Euroopan tietosuojaneuvosto muistuttaa, että sähköisen viestinnän tietosuojadirektiivissä suostumuksella tarkoitetaan samaa kuin tietosuoja-asetuksessa ja että suostumuksen on täytettävä kaikki tietosuoja-asetuksen 4 artiklan 11 kohdassa ja 7 artiklassa vahvistetut suostumuksen edellytykset.

17. Vaikka suostumus on periaatteena, sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaan tietojen tallentaminen tai päätelaitteelle tallennettujen tietojen käyttäminen kuitenkin vapauttaa tietoista suostumusta koskevasta vaatimuksesta, jos tietojen tallentaminen tai käyttäminen täyttää jonkin seuraavista kriteereistä:

    - **poikkeus 1:** sen ainoana tarkoituksena on toteuttaa viestinnän välittäminen sähköisissä viestintäverkoissa;
    - **poikkeus 2:** se on ehdottoman välttämätöntä tietoyhteiskuntapalvelun tarjoajalle sellaisen palvelun tarjoamiseksi, jota tilaaja tai käyttäjä on erityisesti pyytänyt.

18. Tällaisissa tapauksissa henkilötietojen käsittely, mukaan lukien päätelaitteessa sijaitsevien tietojen kautta saatujen henkilötietojen käsittely, perustuu johonkin yleisen tietosuoja-asetuksen 6 artiklassa säädettyyn oikeusperusteeseen. Suostumusta ei tarvita esimerkiksi silloin, kun tietojen käsittely on tarpeen rekisteröidyn pyytämien GPS-navigointipalvelujen tarjoamiseksi, jos tällaiset palvelut voidaan luokitella tietoyhteiskuntapalveluiksi.

1.3 Soveltamisala

19. Euroopan tietosuojaneuvosto haluaa huomauttaa, että näillä ohjeilla on tarkoitus helpottaa kyseisessä ympäristössä toimivien eri sidosryhmien suorittaman henkilötietojen käsittelyn vaatimustenmukaisuutta. Niillä ei kuitenkaan ole tarkoitus kattaa kaikkia mahdollisia asiaan liittyviä käyttötapauksia eikä antaa ohjeita kaikkiin mahdollisiin erityistilanteisiin.

20. Tässä asiakirjassa keskitytään erityisesti henkilötietojen käsittelyyn tilanteessa, jossa rekisteröidyt (esim. kuljettajat, matkustajat, ajoneuvojen omistajat ja muut tienkäyttäjät) käyttävät verkkoon liitettyjä ajoneuvoja muuhun kuin ammatilliseen tarkoitukseen. Asiakirjassa käsitellään erityisesti henkilötietoja, joita i) käsitellään ajoneuvon sisällä, ii) vaihdetaan ajoneuvon ja siihen liitettyjen henkilökohtaisten laitteiden (esim. käyttäjän älypuhelimen) välillä tai iii) kerätään ajoneuvosta paikallisesti ja siirretään ulkopuolisille tahoille (esim. ajoneuvojen valmistajat, infrastruktuurin haltijat, vakuutusyhtiöt, autonkorjaajat) jatkokäsittelyä varten.

21. Verkkoon liitetyt ajoneuvot on tässä asiakirjassa ymmärrettävä käsitteen laajassa merkityksessä. Verkkoon liitetty ajoneuvo voidaan määritellä ajoneuvoksi, joka on

[18] Lausunto 5/2019, kohta 41.

[19] Euroopan tietosuojaneuvoston ohjeet 2/2019 yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä, versio 2.0, 8. lokakuuta 2019, kohta 1.

varustettu useilla elektronisilla ohjausyksiköillä, jotka on yhdistetty toisiinsa ajoneuvoon asennetun verkon kautta, sekä yhteystoiminnoilla, joiden avulla ajoneuvo voi jakaa tietoja muiden sekä ajoneuvon sisällä että sen ulkopuolella olevien laitteiden kanssa. Näin ollen tietoja voidaan vaihtaa ajoneuvon ja siihen kytkettyjen henkilökohtaisten laitteiden välillä esimerkiksi siten, että mobiilisovellukset peilataan auton kojelaudan tieto- ja viihdeyksikköön. Tämän asiakirjan soveltamisalaan kuuluu myös sellaisten erillisten mobiilisovellusten kehittäminen kuljettajan avuksi, jotka ovat riippumattomia ajoneuvosta (niitä käytetään esimerkiksi pelkästään älypuhelimella), koska ne lisäävät ajoneuvon liitettävyysominaisuuksia, vaikka ne eivät välttämättä sinällään perustu tiedonsiirtoon ajoneuvon kanssa. Verkkoon liitettyihin ajoneuvoihin liittyviä sovelluksia on paljon erilaisia, ja niihin voi sisältyä seuraavia ominaisuuksia[20]:

22. *Liikkuvuuden hallinta:* toiminnot, joiden avulla kuljettajat voivat päästä matkakohteeseen nopeasti ja kustannustehokkaasti, sillä ne tarjoavat oikea-aikaista tietoa GPS-navigoinnista, mahdollisesti vaarallisista ympäristöolosuhteista (esim. liukkaat tiet), liikenneruuhkista tai tietöistä, pysäköintialueista tai huoltamoista, optimoidusta polttoaineenkulutuksesta tai tienkäyttömaksuista.

23. *Ajoneuvon hallinta:* toiminnot, joiden on tarkoitus auttaa kuljettajia vähentämään käyttökustannuksia ja helpottamaan käyttöä, kuten ilmoitus ajoneuvon kunnosta ja huoltomuistutukset, käyttötietojen siirtäminen (esim. ajoneuvojen huoltopalveluja varten), räätälöidyt käyttöön perustuvat vakuutukset, etätoiminnot (esim. lämmitysjärjestelmä) tai säädöt (esim. istuimen asento).

24. *Tieliikenneturvallisuus:* toiminnot, jotka varoittavat kuljettajaa ulkoisista vaaroista ja sisäisistä reaktioista, kuten törmäyssuojaus, vaaravaroitukset, kaistavahti, kuljettajan väsymyksen tunnistus, hätäpuhelut (eCall) tai ns. mustat laatikot onnettomuustutkintaa varten (tapahtumien rekisteröintilaite).

25. *Viihde:* toiminnot, jotka tarjoavat kuljettajalle ja matkustajille tietoa viihdettä. Näitä ovat muun muassa älypuhelinten käyttöliittymät (handsfree-puhelut, puheohjatut tekstiviestit), WLAN-tukiasemat, musiikki, videot, internet, sosiaalinen media, mobiilitoimistot tai älykotipalvelut.

26. *Kuljettajan avustaminen:* toiminnot, jotka liittyvät osittain tai kokonaan automatisoituun ajamiseen, kuten toiminnallinen apu tai automaattiohjaus raskaassa liikenteessä, pysäköintialueilla tai moottoriteillä.

27. *Hyvinvointi:* kuljettajan ajomukavuutta, ajokykyä ja -kuntoa seuraavat toiminnot, kuten väsymyksen tunnistaminen tai lääkinnällinen apu.

28. Näin ollen ajoneuvot voivat olla natiivisti verkkoon liitettyjä, ja henkilötietoja voidaan kerätä useilla eri tavoilla, kuten i) ajoneuvoantureilla, ii) telemaattisilla yksiköillä tai iii) mobiilisovelluksilla (esim. kuljettajalle kuuluvalta laitteelta). Jotta mobiilisovellukset kuuluisivat tämän asiakirjan soveltamisalaan, niiden on liityttävä ajoympäristöön. Esimerkiksi GPS-navigointisovellukset kuuluvat soveltamisalaan. Sovellukset, jotka pelkästään ehdottavat kuljettajille kiinnostavia kohteita (ravintolat, historialliset kohteet jne.), eivät kuitenkaan kuulu näiden ohjeiden soveltamisalaan.

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

29. Suuri osa verkkoon liitetyn ajoneuvon tuottamista tiedoista liittyy tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, ja näin ollen ne ovat henkilötietoja. Tietoihin kuuluvat esimerkiksi suoraan tunnistettavissa olevat tiedot (esim. täydelliset tiedot kuljettajan henkilöllisyydestä) sekä välillisesti tunnistettavat tiedot, kuten tiedot tehdyistä matkoista, ajoneuvon käyttötiedot (esim. ajotyyliä tai kuljettua matkaa koskevat tiedot) tai ajoneuvon tekniset tiedot (esim. ajoneuvon osien kulumista koskevat tiedot). Nämä tiedot voidaan yhdistää luonnolliseen henkilöön, kun niitä verrataan muihin tiedostoihin ja erityisesti ajoneuvon valmistenumeroon (VIN). Verkkoon liitettyjen ajoneuvojen henkilötietoihin voi sisältyä myös metadataa, kuten tiedot ajoneuvon huoltostatuksesta. Toisin sanoen kaikki tiedot, jotka voidaan yhdistää luonnolliseen henkilöön, kuuluvat tämän asiakirjan soveltamisalaan.

30. Verkkoon liitettyjen ajoneuvojen ekosysteemiin liittyy useita eri sidosryhmiä. Tarkemmin sanottuna ekosysteemiin kuuluvat autoteollisuuden perinteiset toimijat sekä digitaaliteollisuuden uudet toimijat. Näin ollen nämä ohjeet on suunnattu ajoneuvojen valmistajille, laitevalmistajille ja autoteollisuuden alihankkijoille, autokorjaamoille, autojen jälleenmyyjille, ajoneuvoihin liittyvien palvelujen tarjoajille, ajoneuvokannan hallinnoijille, moottoriajoneuvovakuutuksia tarjoaville vakuutusyhtiöille, viihdepalvelujen tarjoajille, teleoperaattoreille, tieinfrastruktuurin haltijoille ja viranomaisille sekä rekisteröidyille. Euroopan tietosuojaneuvosto korostaa, että rekisteröityjen ryhmät vaihtelevat palvelun mukaan (esim. kuljettajat, omistajat, matkustajat jne.). Tämä luettelo ei ole tyhjentävä, sillä ekosysteemiin kuuluu monenlaisia palveluja, mukaan lukien palvelut, jotka edellyttävät suoraa todentamista tai tunnistamista, ja palvelut, joihin sitä ei tarvita.

31. Osa luonnollisten henkilöiden ajoneuvossa suorittamasta tietojenkäsittelystä tapahtuu ”*yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa*”, minkä vuoksi se ei kuulu yleisen tietosuoja-asetuksen soveltamisalaan.[21] Tämä koskee sellaista ajoneuvossa tapahtuvaa henkilötietojen käsittelyä, jota suorittavat ainoastaan ne rekisteröidyt, jotka ovat toimittaneet kyseiset tiedot ajoneuvon kojelautayksikköön. Euroopan tietosuojaneuvosto muistuttaa kuitenkin, että yleisen tietosuoja-asetuksen johdanto-osan 18 kappaleen mukaan yleistä tietosuoja-asetusta ”*sovelletaan kuitenkin rekisterinpitäjiin tai henkilötietojen käsittelijöihin, jotka tarjoavat keinot tällaiseen henkilökohtaiseen tai kotitaloutta koskevaan henkilötietojen käsittelyyn*”.

1.3.1 Tämän asiakirjan soveltamisalan ulkopuolella

32. Työnantajat, jotka tarjoavat henkilöstölleen työsuhdeautoja, saattavat haluta valvoa työntekijöidensä toimia (esimerkiksi työntekijöiden, tavaroiden tai ajoneuvojen turvallisuuden varmistamiseksi, resurssien kohdentamiseksi, palvelun jäljittämiseksi ja laskuttamiseksi tai työajan tarkistamiseksi). Työnantajien tässä yhteydessä suorittama tietojenkäsittely herättää työsuhteeseen liittyviä erityiskysymyksiä, joita saatetaan säännellä kansallisella tasolla työlainsäädännöllä, jota taas ei voida kuvata tarkemmin näissä ohjeissa.[22]

33. Vaikka ammatillisiin tarkoituksiin käytettävien hyötyajoneuvojen (kuten joukkoliikenteen) sekä yhteiskuljetusten ja liikkuminen palveluna -ratkaisujen (MaaS) yhteydessä tapahtuva tietojenkäsittely saattaa nostaa esiin erityisiä näkökohtia, jotka eivät kuulu näiden yleisten

[21] Ks. yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan c alakohta.
[22] Tietosuojatyöryhmä käsitteli asiaa tietojenkäsittelystä työpaikalla antamassaan lausunnossa 2/2017 (WP249); https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

ohjeiden soveltamisalaan, monia näissä ohjeissa esitettyjä periaatteita ja suosituksia voidaan soveltaa myös tämäntyyppiseen käsittelyyn.

34. Koska verkkoon liitetyt ajoneuvot ovat radiotaajuuksia käyttäviä järjestelmiä, niihin kohdistetaan passiivista seurantaa, kuten seurantaa langattoman verkon tai Bluetooth-yhteyden avulla. Tässä mielessä ne eivät eroa muista verkkoon liitetyistä laitteista, ja ne kuuluvat parhaillaan tarkistettavana olevan sähköisen viestinnän tietosuojadirektiivin soveltamisalaan. Näin ollen tämä sulkee pois myös langattomalla verkolla varustettujen ajoneuvojen laajamittaisen seurannan, joka johtuu siitä, että suuri joukko sivullisia käyttää yleisiä älypuhelinten paikannuspalveluja.[23] Nämä palvelut raportoivat rutiininomaisesti kaikista näkyvistä langattomista verkoista keskuspalvelimille. Koska sisäänrakennettua langatonta yhteyttä voidaan pitää ajoneuvon toissijaisena tunnisteena[24], vaarana on, että ajoneuvojen liikkeestä kootaan järjestelmällisesti ja jatkuvasti kattavia profiileja.

35. Ajoneuvoissa on yhä enemmän kuvan tallennuslaitteita (esim. autojen pysäköintikamerajärjestelmät tai kojelautakamerat). Koska kyse on julkisten tilojen kuvaamisesta, jonka osalta on arvioitava kunkin jäsenvaltion asiaa koskevaa lainsäädäntökehystä, tällainen tietojenkäsittely ei kuulu näiden ohjeiden soveltamisalaan.

36. Direktiivin 2010/40/EU[25] määritelmän mukaiset vuorovaikutteiset älykkäät liikennejärjestelmät (C-ITS-järjestelmät) mahdollistavaa tietojenkäsittelyä on käsitelty 29 artiklan mukaisen tietosuojatyöryhmän asiasta laatimassa lausunnossa[26]. Vaikka direktiivissä annettuun C-ITS-järjestelmän määritelmään ei sisälly teknisiä eritelmiä, 29 artiklan mukainen tietosuojatyöryhmä keskittyy lausunnossaan lyhyen kantaman viestintään, eli siinä ei käsitellä verkko-operaattorin toimintaa. Tarkemmin sanottuna siinä analysoidaan erityisiä käyttötapauksia, jotka on kehitetty alkuvaiheen käyttöönottoa varten, ja siinä sitouduttiin arvioimaan myöhemmin uusia kysymyksiä, joita epäilemättä tulee esiin, kun automaatiota lisätään. Koska C-ITS-järjestelmien tietosuojavaikutukset ovat hyvin erityislaatuisia (sijaintitietojen ennennäkemättömät määrät, henkilötietojen jatkuva lähettäminen, ajoneuvojen ja muiden tieinfrastruktuuripalvelujen välinen tietojenvaihto jne.) ja koska niistä keskustellaan edelleen Euroopan tasolla, tällainen henkilötietojen käsittely ei kuulu näiden ohjeiden soveltamisalaan.

37. Lopuksi Euroopan tietosuojaneuvosto toteaa, että tässä asiakirjassa ei ole tarkoitus käsitellä kaikkia verkkoon liitettyihin ajoneuvoihin mahdollisesti liittyviä kysymyksiä, joten sitä ei voida pitää tyhjentävänä.

1.4 Määritelmät

[23] Lisätietoja: 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 ja Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nizza, Ranska, 23.–27. heinäkuuta 2017, s. 32–37.

[25] Direktiivi 2010/40/EU, annettu 7 päivänä heinäkuuta 2010, tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista; https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32010L0040

[26] Tietosuojatyöryhmän lausunto 3/2017 henkilötietojen käsittelystä vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) yhteydessä; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

38. Henkilötietojen **käsittelyllä** tarkoitetaan kaikenlaisia henkilötietoihin liittyviä toimintoja, joita ovat muun muassa tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, tutkiminen, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen taikka rajoittaminen, poistaminen tai tuhoaminen.[27]

39. **Rekisteröity** on luonnollinen henkilö, johon käsiteltävät tiedot liittyvät. Verkkoon liitettyjen ajoneuvojen osalta rekisteröity voi olla erityisesti kuljettaja (pääasiallinen tai satunnainen), matkustaja tai ajoneuvon omistaja.[28]

40. **Rekisterinpitäjä** on henkilö, joka määrittelee verkkoon liitetyissä ajoneuvoissa suoritettavan henkilötietojen käsittelyn tarkoitukset ja keinot.[29] Rekisterinpitäjiä voivat olla palveluntarjoajat, jotka käsittelevät ajoneuvotietoja liikennetietojen, taloudellista ajoa koskevien viestien tai ajoneuvon toimintaa koskevien hälytysten lähettämiseksi kuljettajalle, vakuutusyhtiöt, jotka tarjoavat käyttöön perustuvia ”*Pay As You Drive*” -sopimuksia, tai ajoneuvojen valmistajat, jotka keräävät ajoneuvon osien kulumista koskevia tietoja sen laadun parantamiseksi. Yleisen tietosuoja-asetuksen 26 artiklan mukaan vähintään kaksi rekisterinpitäjää voi yhdessä määrittää käsittelyn tarkoitukset ja keinot, ja tällöin niitä pidetään yhteisrekisterinpitäjinä. Tässä tapauksessa niiden on määriteltävä selkeästi omat vastuualueensa, erityisesti siltä osin kuin on kyse rekisteröidyn oikeuksien käytöstä ja yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaisten tietojen toimittamisesta.

41. **Henkilötietojen käsittelijä** on kuka tahansa henkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.[30] Henkilötietojen käsittelijä kerää ja käsittelee tietoja rekisterinpitäjän ohjeiden mukaisesti käyttämättä näitä tietoja omiin tarkoituksiinsa. Esimerkiksi useissa tapauksissa laitevalmistajat ja autoteollisuuden alihankkijat voivat käsitellä tietoja ajoneuvojen valmistajien puolesta (mikä ei tarkoita, että ne eivät voi olla rekisterinpitäjiä muiden tarkoitusten osalta). Yleisen tietosuoja-asetuksen 28 artiklassa edellytetään, että henkilötietojen käsittelijät panevat täytäntöön riittävät tekniset ja organisatoriset toimet, jotta voidaan taata riskin kannalta asianmukainen turvallisuustaso, ja siinä säädetään henkilötietojen käsittelijöiden velvollisuuksista.

42. **Vastaanottaja** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei.[31] Esimerkiksi palveluntarjoajan kaupallinen kumppani, joka saa palveluntarjoajalta ajoneuvosta saatuja henkilötietoja, on henkilötietojen vastaanottaja. Riippumatta siitä, toimiiko vastaanottaja uutena rekisterinpitäjänä vai henkilötietojen käsittelijänä, sen on noudatettava kaikkia yleisessä tietosuoja-asetuksessa säädettyjä velvoitteita.

43. Viranomaisia, jotka mahdollisesti saavat henkilötietoja tietyn tutkimuksen puitteissa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti ei kuitenkaan pidetä vastaanottajina[32]; näiden viranomaisten on käsiteltävä kyseisiä tietoja sovellettavia

[27] Ks. yleisen tietosuoja-asetuksen 4 artiklan 2 kohta.
[28] Ks. yleisen tietosuoja-asetuksen 4 artiklan 1 kohta.
[29] Ks. yleisen tietosuoja-asetuksen 4 artiklan 7 kohta ja Euroopan tietosuojaneuvoston ohjeet 7/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa (jäljempänä ’ohjeet 7/2020’).
[30] Ks. yleisen tietosuoja-asetuksen 4 artiklan 8 kohta ja ohjeet 7/2020.
[31] Ks. yleisen tietosuoja-asetuksen 4 artiklan 9 kohta ja ohjeet 7/2020.
[32] Yleisen tietosuoja-asetuksen 4 artiklan 9 kohta ja johdanto-osan 31 kappale.

tietosuojasääntöjä noudattaen käsittelyn tarkoitusten mukaisesti. Esimerkiksi lainvalvontaviranomaiset ovat valtuutettuja kolmansia osapuolia, kun ne pyytävät henkilötietoja osana Euroopan unionin tai jäsenvaltion lainsäädännön mukaista tutkintaa.

1.5 Yksityisyyden suojaa ja tietosuojaa koskevat riskit

44. Tietosuojatyöryhmä on tuonut esiin useita huolenaiheita, joita liittyy esineiden internetin järjestelmiin, joita voidaan soveltaa myös verkkoon liitettyihin ajoneuvoihin.[33] Tietoturvaan ja valvontaan liittyvät kysymykset, joita on jo painotettu esineiden internetin osalta, ovat verkkoon liitettyjen ajoneuvojen osalta vieläkin arkaluonteisempia, koska niihin liittyy liikenneturvallisuuteen liittyviä huolenaiheita ja ne voivat vaikuttaa kuljettajan fyysiseen koskemattomuuteen ympäristössä, jota perinteisesti pidetään eristettynä ja suojattuna ulkoisilta häiriöiltä.

45. Verkkoon liitettyihin ajoneuvoihin liittyy myös merkittäviä sijaintitietojen käsittelyyn liittyvää tietosuojaa ja yksityisyyttä koskevia huolia, koska niiden yhä tungettelevampi luonne voi heikentää nykyisiä mahdollisuuksia pysyä anonyymina. Euroopan tietosuojaneuvosto haluaa painottaa erityisesti sitä, että paikannusteknologian käyttö edellyttää erityisten suojatoimien toteuttamista yksilöiden valvonnan ja tietojen väärinkäytön estämiseksi, ja lisätä sidosryhmien tietoisuutta asiasta.

1.5.1 Hallinnan puute ja tietojen epäsymmetria

46. Ajoneuvojen kuljettajille ja matkustajille ei välttämättä aina anneta riittävästi tietoa tietojen käsittelystä verkkoon liitetyssä ajoneuvossa tai sen välityksellä. Tiedot voidaan antaa ainoastaan ajoneuvon omistajalle, joka ei välttämättä ole kuljettaja, eikä tietoja välttämättä anneta oikea-aikaisesti. Näin ollen vaarana on, että tarvittavaan hallintaan ei ole käytettävissä riittäviä toimintoja tai vaihtoehtoja, jotta asianomaiset henkilöt voisivat käyttää tietosuojaa ja yksityisyyttä koskevia oikeuksiaan. Tämä seikka on tärkeä, koska ajoneuvot voivat elinkaarensa aikana kuulua useammalle kuin yhdelle omistajalle joko siksi, että ne myydään, tai siksi, että ne on vuokrattu ostamisen sijaan.

47. Myös ajoneuvossa tapahtuva viestintä voi käynnistyä itsestään ja käyttäjän suunnittelematta, ilman että henkilö on siitä tietoinen. Koska ajoneuvon ja siihen liitettyjen laitteiden vuorovaikutusta ei ole mahdollista valvoa tehokkaasti, käyttäjän on äärimmäisen vaikeaa valvoa tietovirtaa. Vieläkin vaikeampaa on hallita sen myöhempää käyttöä ja estää mahdollista käyttöä muuhun kuin alkuperäiseen tarkoitukseen.

1.5.2 Käyttäjän suostumuksen laatu

48. Euroopan tietosuojaneuvosto korostaa, että kun tietojenkäsittely perustuu suostumukseen, kaikki pätevän suostumuksen osatekijät on täytettävä, mikä tarkoittaa Euroopan tietosuojaneuvoston suostumusta koskevien suuntaviivojen[34] tulkinnan mukaan, että suostumuksen on oltava vapaaehtoinen, yksilöity ja tietoinen ja se on rekisteröidyn yksiselitteinen tahdonilmaisu. Rekisterinpitäjien on kiinnitettävä erityistä huomiota yksityiskohtaisiin sääntöihin, jotka koskevat pätevän suostumuksen saamista eri osapuolilta, kuten autonomistajilta tai auton käyttäjiltä. Tällainen suostumus on annettava erikseen tiettyjä tarkoituksia varten, eikä sitä voi liittää uuden auton osto- tai vuokrasopimukseen. Suostumus on voitava peruuttaa yhtä helposti kuin se annetaan.

49. Tätä on sovellettava myös silloin, kun suostumus edellyttää sähköisen viestinnän tietosuojadirektiivin noudattamista, esimerkiksi jos tietoja tallennetaan tai ajoneuvoon

[33] Tietosuojatyöryhmän lausunto 8/2014 esineiden internetin viimeaikaisesta kehityksestä; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_fi.pdf

[34] Euroopan tietosuojaneuvoston asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat 5/2020, versio 1.1, 4. toukokuuta 2020 (jäljempänä ’suuntaviivat 5/2020’).

tallennettuja tietoja käytetään, kuten sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa edellytetään. Kuten edellä on esitetty, suostumusta on tässä yhteydessä tulkittava yleisen tietosuoja-asetuksen perusteella.

50. Monissa tapauksissa käyttäjä ei välttämättä ole tietoinen ajoneuvossaan suoritetusta tietojenkäsittelystä. Tällainen tiedonpuute muodostaa merkittävän esteen yleisen tietosuoja-asetuksen mukaisen pätevän suostumuksen osoittamiselle, koska suostumuksen on oltava tietoinen. Tällaisissa tapauksissa suostumusta ei voida käyttää yleisen tietosuoja-asetuksen mukaisena oikeusperusteena tietojen käsittelylle.

51. Perinteisiä tapoja, joita käytetään henkilön suostumuksen hankkimiseen, voi olla vaikea soveltaa verkkoon liitettyjen ajoneuvojen tapauksessa, mistä seuraa sellaisen laadultaan heikon suostumuksen saaminen, joka perustuu puutteellisiin tietoihin tai siihen, että yksilöiden ilmaisemien mieltymysten mukaista nimenomaista suostumusta on todellisuudessa mahdotonta antaa. Käytännössä suostumuksen saaminen voi olla vaikeaa myös sellaisilta kuljettajilta ja matkustajilta, jotka eivät ole sidoksissa ajoneuvon omistajaan, kun kyseessä on käytetty, leasingvuokrattu, vuokrattu tai lainattu ajoneuvo.

52. Jos sähköisen viestinnän tietosuojadirektiivissä ei edellytetä rekisteröidyn suostumusta, rekisterinpitäjän on kuitenkin valittava yleisen tietosuoja-asetuksen 6 artiklan mukainen oikeusperuste, joka soveltuu kyseiseen henkilötietojen käsittelyyn parhaiten.

1.5.3 Henkilötietojen myöhempi käsittely

53. Kun tiedot kerätään sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa edellytetyn suostumuksen tai jonkin 5 artiklan 3 kohdassa säädetyn poikkeuksen perusteella ja niitä käsitellään myöhemmin yleisen tietosuoja-asetuksen 6 artiklan mukaisesti, niitä voidaan käsitellä myöhemmin vain, jos rekisterinpitäjä pyytää tähän muuhun tarkoitukseen uutta suostumusta tai jos rekisterinpitäjä voi osoittaa, että käsittely perustuu unionin tai jäsenvaltion lainsäädäntöön yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi.[35] Tietosuojaneuvosto katsoo, että myöhempi käsittely yleisen tietosuoja-asetuksen 6 artiklan 4 kohdan mukaisen yhteensopivuustestin perusteella ei ole mahdollista tällaisissa tapauksissa, koska se heikentäisi sähköisen viestinnän tietosuojadirektiivissä säädettyä tietosuojan tasoa. Sähköisen viestinnän tietosuojadirektiivissä edellytettävän suostumuksen on oltava yksilöity ja tietoinen, mikä tarkoittaa, että rekisteröityjen on oltava tietoisia kunkin tietojenkäsittelyn tarkoituksesta ja heillä on oltava oikeus kieltäytyä tietyistä tarkoituksista.[36] Jos myöhempi käsittely yleisen tietosuoja-asetuksen 6 artiklan 4 kohdan mukaisen yhteensopivuustestin perusteella olisi mahdollista, voitaisiin nykyisessä direktiivissä asetettujen suostumusta koskevien vaatimusten periaate kiertää.

54. Euroopan tietosuojaneuvosto muistuttaa, että alkuperäinen suostumus ei koskaan oikeuta myöhempää käsittelyä, koska suostumuksen on oltava tietoon perustuva ja erityinen, jotta se olisi pätevä.

55. Esimerkiksi ajoneuvon käytön aikana huoltotarkoituksiin kerättyjä etämittaustietoja ei saa ilman käyttäjän suostumusta antaa liikennevakuutusyhtiöille ilman, että käyttäjät antavat

[35] Katso myös Euroopan tietosuojaneuvoston ohjeet 10/2020 yleisen tietosuoja-asetuksen 23 artiklan mukaisista rajoituksista.
[36] Suuntaviivat 5/2020, kohdat 3.2 ja 3.3.

suostumuksensa kuljettajaprofiilien luomiseen ajokäyttäytymiseen perustuvien vakuutusten tarjoamista varten.

56. Lisäksi lainvalvontaviranomaiset voivat käsitellä verkkoon liitettyjen ajoneuvojen keräämiä tietoja ylinopeuden tai muiden rikkomusten havaitsemiseksi, jos ja kun lainvalvontadirektiivissä asetetut erityisehdot täyttyvät. Tässä tapauksessa tällaisten tietojen katsotaan liittyvän rikostuomioihin ja rikkomuksiin yleisen tietosuoja-asetuksen 10 artiklassa ja sovellettavassa kansallisessa lainsäädännössä säädettyjen edellytysten mukaisesti. Valmistajat voivat toimittaa lainvalvontaviranomaisille tällaisia tietoja, jos kyseisenlaista käsittelyä koskevat erityisedellytykset täyttyvät. Tietosuojaneuvosto huomauttaa, että henkilötietojen käsittely yksinomaan lainvalvontaviranomaisten esittämien pyyntöjen täyttämiseksi ei ole yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohdassa tarkoitettu tietty, nimenomainen ja laillinen tarkoitus. Kun lainvalvontaviranomaisilla on lainsäädännön mukainen oikeus käsitellä tietoja, ne voivat olla yleisen tietosuoja-asetuksen 4 artiklan 10 kohdassa tarkoitettuja kolmansia osapuolia. Tällöin valmistajilla olisi oikeus antaa niille kaikki käytettävissään olevat tiedot edellyttäen, että kunkin jäsenvaltion asiaa koskevaa oikeudellista kehystä noudatetaan.

1.5.4 Liiallinen tiedonkeruu

57. Koska verkkoon liitetyissä ajoneuvoissa käytetään yhä enemmän antureita, suurena vaarana on, että tietoa kerätään liikaa verrattuna siihen, mikä on tarpeen tavoitteen saavuttamiseksi.

58. Uusien ja erityisesti koneoppimisalgoritmeihin perustuvien toimintojen kehittäminen saattaa edellyttää suurta määrää tietoa, jota on kerätty pitkän ajanjakson aikana.

1.5.5 Henkilötietojen turvallisuus

59. Verkkoon liitetyissä ajoneuvoissa on useita eri toimintoja, palveluja ja käyttöliittymiä (esim. internet, USB, RFID, langaton verkko), ja tästä syystä niissä on runsaasti hyökkäyskohteita ja näin ollen mahdollisia haavoittuvuuksia, joiden kautta henkilötiedot voivat vaarantua. Toisin kuin useimmat esineiden internetin laitteet, verkkoon liitetyt ajoneuvot ovat kriittisiä järjestelmiä, joissa tietoturvaloukkaus voi vaarantaa käyttäjien ja ympärillä olevien ihmisten hengen. Näin ollen on entistä tärkeämpää puuttua siihen riskiin, että hakkerit yrittävät hyödyntää verkkoon liitettyjen ajoneuvojen haavoittuvuutta.

60. Lisäksi ajoneuvoihin ja/tai ulkoisiin kohteisiin (esim. pilvipalveluinfrastruktuureihin) tallennetut henkilötiedot on suojattava asianmukaisesti luvattomalta käytöltä. Ajoneuvo on esimerkiksi luovutettava huollon ajaksi teknikolle, joka tarvitsee käyttöönsä osan ajoneuvon teknisistä tiedoista. Vaikka teknikon on päästävä käsiksi teknisiin tietoihin, hän saattaa yrittää käyttää kaikkia ajoneuvoon tallennettuja tietoja.

2 YLEISET SUOSITUKSET

61. Edellä kuvattujen rekisteröityihin kohdistuvien riskien lieventämiseksi ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien tai muiden sidosryhmien, jotka voivat toimia verkkoon liitettyjen ajoneuvojen rekisterinpitäjänä tai henkilötietojen käsittelijänä, olisi noudatettava seuraavia yleisiä suosituksia.

2.1 Tietojen ryhmät

62. Kuten johdannossa todettiin, useimmat verkkoon liitettyihin ajoneuvoihin liittyvät tiedot katsotaan henkilötiedoiksi siltä osin kuin ne voidaan yhdistää yhteen tai useampaan tunnistettavissa olevaan henkilöön. Tällaisia tietoja ovat tekniset tiedot ajoneuvon liikkeistä (esim. nopeus, kuljettu matka) sekä ajoneuvon kunnosta (esim. moottorin jäähdytysnesteen lämpötila, moottorin käyntinopeus ja rengaspaine). Tiettyihin verkkoon liitettyjen ajoneuvojen tuottamiin tietoihin voi myös olla syytä kiinnittää erityistä huomiota, kun otetaan huomioon niiden arkaluonteisuus ja/tai mahdolliset vaikutukset rekisteröityjen oikeuksiin ja etuihin. Toistaiseksi Euroopan tietosuojaneuvosto on yksilöinyt kolme henkilötietojen ryhmää, joihin ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien on kiinnitettävä erityistä huomiota: sijaintitiedot, biometriset tiedot (ja yleisen tietosuoja-asetuksen 9 artiklassa määritellyt erityiset henkilötietoryhmät) ja tiedot, jotka voivat paljastaa sääntöjenvastaisuuksia tai liikennerikkomuksia.

2.1.1 Sijaintitiedot

63. Ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien olisi henkilötietoja kerätessään muistettava, että sijaintitiedot paljastavat erityisen paljon tietoa rekisteröidyn elämäntavasta. Tehtyjen matkojen perusteella voidaan tyypillisesti päätellä kuljettajan työpaikka ja asuinpaikka sekä kuljettajan kiinnostuksen kohteet (vapaa-aika) ja mahdollisesti paljastaa arkaluonteisia tietoja. Esimerkiksi henkilön uskonto voidaan päätellä uskonnonharjoituspaikan perusteella ja seksuaalinen suuntautuminen vierailtujen kohteiden perusteella. Näin ollen ajoneuvon ja laitteiden valmistajan, palveluntarjoajan ja muun rekisterinpitäjän olisi oltava erityisen tarkkoja siitä, että sijaintitietoja ei kerätä, paitsi jos se on käsittelyn kannalta ehdottoman välttämätöntä. Esimerkiksi silloin, kun käsittelyyn sisältyy ajoneuvon liikkeen havaitseminen, tähän tarkoitukseen riittää gyroskooppi, eikä sijaintitietoja tarvitse kerätä.

64. Sijaintitietojen keräämisessä on yleensä noudatettava myös seuraavia periaatteita:

- Kerättävien sijaintitietojen käyttötiheys ja yksityiskohtaisuus määritetään asianmukaisesti käsittelyn tarkoituksen mukaan. Esimerkiksi sääsovellus ei saisi käyttää ajoneuvon sijaintitietoja jatkuvasti edes rekisteröidyn suostumuksella.
- Käsittelyn tarkoituksesta annetaan täsmälliset tiedot (Onko sijaintihistoria tallennettu? Jos on, mihin tarkoitukseen?).
- Jos käsittely perustuu suostumukseen, hankitaan pätevä (vapaaehtoinen, yksilöity ja tietoinen) suostumus, joka erottuu yleisistä myynti- tai käyttöehdoista (esimerkiksi kojelautatietokoneessa).
- Paikannus aktivoidaan vain silloin, kun käyttäjä käynnistää toiminnon, joka edellyttää tietoa ajoneuvon sijainnista, eikä oletusarvoisesti ja jatkuvasti, kun auto käynnistetään.
- Käyttäjälle ilmoitetaan paikannuksen aktivoinnista erityisesti kuvakkeiden avulla (esim. näytöllä liikkuva nuoli).
- Paikannus on mahdollista poistaa käytöstä milloin tahansa.
- Tietoja säilytetään rajoitetun ajan.

2.1.2 Biometriset tiedot

65. Verkkoon liitettyjen ajoneuvojen osalta luonnollisen henkilön yksiselitteistä tunnistamista varten käytettäviä biometrisiä tietoja voidaan käsitellä yleisen tietosuoja-asetuksen

9 artiklan ja kansallisten poikkeusten sallimissa rajoissa muun muassa ajoneuvoon pääsyn mahdollistamiseksi, kuljettajan/omistajan tunnistamiseksi ja/tai kuljettajan profiiliasetusten käyttämiseksi. Harkittaessa biometristen tietojen käyttöä sen takaaminen, että rekisteröity voi hallita tietojaan täysin, edellyttää toisaalta muun kuin biometrisen vaihtoehdon tarjoamista (esim. fyysisen avaimen tai koodin käyttö) ilman lisärajoituksia (eli biometrisen tunnisteen käytön ei pitäisi olla pakollista) ja toisaalta biometrisen mallin tallentamista ja vertailua salatussa muodossa ainoastaan paikallisesti siten, että biometrisiä tietoja ei käsitellä ulkoisessa luku-/vertailupäätteessä.

66. Biometristen tietojen[37] osalta on tärkeää varmistaa, että biometrisen tunnistuksen ratkaisu on riittävän luotettava ja että se vastaa erityisesti seuraavia periaatteita:

- Käytössä oleva biometrinen ratkaisu (esim. väärien positiivisten ja väärien negatiivisten tulosten määrä) mukautetaan vaaditun kulunvalvonnan turvallisuustasoon.
- Käytetty biometrinen ratkaisu perustuu sensoriin, joka kestää hyökkäyksiä (esim. sormenjälkitunnistuksessa käytetään tasaista painallusta).
- Todennusyritysten määrä on rajallinen.
- Biometrinen malli tallennetaan ajoneuvoon salatussa muodossa salausalgoritmin ja uusimman tekniikan mukaisen avainten hallinnan avulla.
- Biometrisen mallin muodostamiseen ja käyttäjien todentamiseen käytettävät raakatiedot käsitellään reaaliajassa niin, että niitä ei tallenneta edes paikallisesti.

2.1.3 Rikoksen tai muun rikkomuksen paljastavat tiedot

67. Jotta voidaan käsitellä tietoja, jotka liittyvät yleisen tietosuoja-asetuksen 10 artiklassa tarkoitettuihin mahdollisiin rikoksiin, tietosuojaneuvosto suosittelee tietojen paikallista käsittelyä, jotta kyseinen käsittely on täysin rekisteröidyn hallinnassa (ks. kohta 2.4, jossa käsitellään paikallista käsittelyä). Joitakin poikkeuksia lukuun ottamatta (ks. jäljempänä kohdassa 3.3 esitetty onnettomuustutkimuksia koskeva esimerkkitapaus) rikoksen tai muun rikkomuksen paljastavien tietojen ulkoinen käsittely on kiellettyä. Tietojen arkaluonteisuuden vuoksi on otettava käyttöön kohdassa 2.7 kuvatun kaltaisia vahvoja suojaamistoimia, jotta voidaan tarjota suoja kyseisten tietojen laitonta käyttöä, muuttamista ja poistamista vastaan.

68. Jotkin verkkoon liitettyjen ajoneuvojen henkilötietojen ryhmät voivat paljastaa, että rikos tai muu rikkomus on tehty tai on tekeillä (rikoksiin liittyvät tiedot), minkä vuoksi niihin sovelletaan erityisiä rajoituksia (esim. tiedot, jotka osoittavat, että ajoneuvo ylitti valkoisen viivan, ajoneuvon hetkellinen nopeus yhdistettynä täsmällisiin sijaintitietoihin). Erityisesti siinä tapauksessa, että toimivaltaiset kansalliset viranomaiset käsittelevät tällaisia tietoja rikostutkintaa ja syytetoimia varten, sovelletaan yleisen tietosuoja-asetuksen 10 artiklassa säädettyjä suojatoimia.

2.2 Tarkoitukset

69. Henkilötietoja voidaan verkkoon liitettyjen ajoneuvojen yhteydessä käsitellä moniin eri tarkoituksiin, jotka liittyvät kuljettajien turvallisuuteen, vakuutuksiin, tehokkaaseen kuljetukseen, viihdepalveluihin tai tietopalveluihin. Yleisen tietosuoja-asetuksen mukaan

[37] Yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa säädetty kielto koskee ainoastaan biometristen tietojen käsittelyä ”*henkilön yksiselitteistä tunnistamista varten*”.

rekisterinpitäjien on varmistettava, että tietoja käsitellään ”tiettyä, nimenomaista ja laillista” tarkoitusta varten, että niitä ei käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla ja että käsittelylle on olemassa voimassa oleva oikeusperuste, kuten yleisen tietosuoja-asetuksen 5 artiklassa edellytetään. Näiden ohjeiden osassa III käsitellään joitakin konkreettisia esimerkkejä tarkoituksista, joita varten verkkoon liitettyihin ajoneuvoihin liittyvät rekisterinpitäjät voivat tietoja käsitellä, ja annetaan kutakin käsittelytyyppiä koskevia erityisiä suosituksia.

2.3 Merkityksellisyys ja tietojen minimointi

70. Tietojen minimoinnin periaatteen[38] noudattamiseksi ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien olisi kiinnitettävä erityistä huomiota tietoryhmiin, joita ne tarvitsevat verkkoon liitetystä ajoneuvosta, koska ne voivat kerätä ainoastaan käsittelyn kannalta merkityksellisiä ja tarpeellisia henkilötietoja. Esimerkiksi sijaintitiedot ovat erityisen tunkeilevia, ja ne voivat paljastaa monenlaista tietoa rekisteröityjen elämästä ja tottumuksia. Näin ollen alan toimijoiden olisi oltava erityisen tarkkoja siitä, että sijaintitietoja ei kerätä, paitsi jos se on käsittelyn kannalta ehdottoman välttämätöntä (ks. edellä kohta 2.1, jossa käsitellään sijaintitietoja).

2.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

71. Kun otetaan huomioon verkkoon liitettyjen ajoneuvojen tuottamien henkilötietojen määrä ja moninaisuus, Euroopan tietosuojaneuvosto toteaa, että rekisterinpitäjien on varmistettava, että verkkoon liitettyjen ajoneuvojen yhteydessä käytettävät teknologiat konfiguroidaan siten, että yksilöiden yksityisyyttä kunnioitetaan ja että yleisen tietosuoja-asetuksen 25 artiklassa edellytettyjä sisäänrakennetun ja oletusarvoisen tietosuojan velvoitteita noudatetaan. Teknologioissa olisi pyrittävä minimoimaan henkilötietojen keruu, tarjoamaan yksityisyyden suojaa suojaavia oletusasetuksia ja varmistamaan, että rekisteröidyllä on asianmukaiset tiedot ja että he voivat muuttaa henkilötietoihinsa liittyviä asetuksia helposti. Erityiset ohjeet siitä, miten valmistajat ja palveluntarjoajat voivat noudattaa sisäänrakennettua ja oletusarvoista tietosuojaa, voisivat olla hyödyllisiä alan toimijoille ja sovellusten tarjoajille.

72. Tietyt jäljempänä kuvatut yleiset käytännöt voivat myös auttaa lieventämään verkkoon liitettyihin ajoneuvoihin liittyvien luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä.[39]

2.4.1 Henkilötietojen paikallinen käsittely

73. Yleisesti ottaen ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien olisi mahdollisuuksien mukaan käytettävä prosesseja, joihin ei liity henkilötietoja tai henkilötietojen siirtämistä ajoneuvon ulkopuolelle (eli tietoja käsitellään sisäisesti). Verkkoon liitettyihin ajoneuvoihin liittyy kuitenkin riskejä, kuten mahdollisuus siihen, että ulkopuoliset toimijat murtautuvat paikalliseen tietojenkäsittelyprosessiin tai paikalliset tiedot vuotavat, kun ajoneuvon osia myydään. Asiaan olisi siis kiinnitettävä asianmukaista huomiota ja on toteutettava riittävät turvatoimet sen varmistamiseksi, että paikallinen käsittely pysyy paikallisena. Tämän skenaarion etuna on, että käyttäjälle taataan hänen henkilötietojensa yksinomainen ja täysi hallinta. Kun tietosuoja on sisäänrakennettua, käsittelyyn liittyy vähemmän yksityisyyden suojaa koskevia riskejä,

[38] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohta.

[39] Katso myös Euroopan tietosuojaneuvoston ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, versio 2.0, annettu 20. lokakuuta 2020 (jäljempänä ’ohjeet 4/2019’).

erityisesti kun sidosryhmiä kielletään käsittelemästä tietoja ilman, että rekisteröity on tästä tietoinen. Näin voidaan myös käsitellä arkaluonteisia tietoja, kuten biometrisiä tietoja tai rikoksiin tai muihin rikkomuksiin liittyviä tietoja sekä yksityiskohtaisia sijaintitietoja, joihin muutoin sovellettaisiin tiukempia sääntöjä (ks. jäljempänä). Vastaavasti tällaiseen käsittelyyn liittyy vähemmän kyberturvallisuusriskejä ja vain vähän viivettä, minkä vuoksi se soveltuu erityisen hyvin automatisoituihin ajoaputoimintoihin. Esimerkkejä tämäntyyppisestä ratkaisusta voisivat olla esimerkiksi seuraavat:

- taloudelliseen ajoon liittyvät sovellukset, joissa käsitellään ajoneuvossa olevia tietoja, jotta ajoneuvon näyttöruudulla voidaan esittää reaaliaikaisesti taloudellista ajoa koskevia ohjeita;

- sovellukset, joissa henkilötietoja siirretään älypuhelimen kaltaiseen laitteeseen niin, että käyttäjä hallitsee siirtoa täysin (esimerkiksi Bluetooth-yhteyden tai langattoman verkon välityksellä), ja joissa ajoneuvon tietoja ei siirretä sovellusten tarjoajille tai ajoneuvojen valmistajille; tähän sisältyisi esimerkiksi älypuhelinten liittäminen auton näytön ja multimediajärjestelmien, mikrofonin (tai muiden anturien) käyttämiseksi puheluja ym. varten, jos kerätyt tiedot pysyvät rekisteröidyn hallinnassa ja niitä käytetään yksinomaan rekisteröidyn pyytämän palvelun tarjoamiseen;

- ajoneuvon sisäiset turvallisuutta parantavat sovellukset, kuten sovellukset, jotka tuottavat äänimerkin tai ohjauspyörän värinää, kun kuljettaja ohittaa auton ilmaisematta suuntaa tai kulkee valkoisten viivojen yli, tai varoittaa ajoneuvon tilasta (esim. varoitus jarrulevyjen kulumisesta);

- ajoneuvon lukituksen avaamiseen, käynnistämiseen ja/tai ajoneuvon tiettyjen komentojen aktivointiin käytettävät sovellukset, joissa käytetään ajoneuvoon tallennettuja kuljettajan biometrisiä tietoja (kuten kasvo- tai äänimalleja tai sormenjälkiä).

74. Edellä mainitun kaltaisiin sovelluksiin liittyy luonnollisen henkilön suorittamaa henkilötietojen käsittelyä toiminnassa, joka on yksinomaan henkilökohtaista tai kotitaloutta koskevaa toimintaa (eli henkilötietoja ei siirretä rekisterinpitäjälle tai henkilötietojen käsittelijälle). Näin ollen **nämä sovellukset jäävät** yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan mukaisesti **yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle**.

75. Vaikka yleistä tietosuoja-asetusta ei sovelleta luonnollisen henkilön suorittamaan henkilötietojen käsittelyyn toiminnassa, joka on yksinomaan henkilökohtaista tai kotitaloutta koskevaa toimintaa, sitä sovelletaan kuitenkin yleisen tietosuoja-asetuksen johdanto-osan 18 kappaleen mukaisesti rekisterinpitäjiin tai henkilötietojen käsittelijöihin, jotka tarjoavat keinot henkilötietojen käsittelyyn tällaista henkilökohtaista tai kotitaloutta koskevaa toimintaa varten (autonvalmistaja, palveluntarjoaja jne.). Näin ollen rekisterinpitäjinä tai henkilötietojen käsittelijöinä toimiessaan niiden on kehitettävä turvallinen autosovellus noudattaen sisäänrakennetun ja oletusarvoisen yksityisyyden suojan periaatetta. Yleisen tietosuoja-asetuksen johdanto-osan 78 kappaleessa säädetään joka tapauksessa, että ”*kehitettäessä, suunniteltaessa, valittaessa ja käytettäessä sovelluksia, palveluja ja tuotteita, jotka perustuvat henkilötietojen käsittelyyn tai käsittelevät henkilötietoja tehtävänsä täyttämiseksi, tuotteiden, palvelujen ja sovellusten tuottajia olisi kannustettava ottamaan huomioon oikeus tietosuojaan niiden kehittäessä ja suunnitellessa tällaisia tuotteita, palveluja ja sovelluksia ja varmistamaan uusin tekniikka asianmukaisesti huomioon ottaen, että rekisterinpitäjät ja henkilötietojen käsittelijät*

pystyvät täyttämään tietosuojavelvoitteensa".[40] Näin voidaan edistää käyttäjäkeskeisten palvelujen kehittämistä ja toisaalta helpottaa ja turvata tulevaisuudessa mahdollisia muita käyttötarkoituksia, jotka voisivat kuulua yleisen tietosuoja-asetuksen soveltamisalaan. Tietosuojaneuvosto suosittelee erityisesti sellaisen turvallisen ajoneuvosovellusalustan kehittämistä, joka on fyysisesti erotettu ajoneuvon turvallisuuden kannalta merkityksellisistä toiminnoista, jotta auton tietojen saatavuus ei riipu tarpeettomista ulkoisista pilvipalveluista.

76. Autonvalmistajien ja palveluntarjoajien olisi mahdollisuuksien mukaan harkittava paikallista tietojenkäsittelyä pilvikäsittelyn mahdollisten riskien lieventämiseksi, kuten tietosuojatyöryhmän tietotekniikan resurssipalveluja koskevassa lausunnossa[41] korostetaan.

77. Yleisesti ottaen käyttäjien olisi voitava valvoa, miten heidän tietojaan kerätään ja käsitellään ajoneuvossa:

- käsittelyä koskevat tiedot on annettava kuljettajan kielellä (käyttöopas, asetukset jne.);
- Euroopan tietosuojaneuvosto suosittelee, että oletusarvoisesti käsitellään vain ajoneuvon toiminnan kannalta ehdottoman välttämättömiä tietoja. Rekisteröidyillä olisi oltava mahdollisuus käynnistää tietojen käsittely tai poistaa se käytöstä kunkin muun tarkoituksen ja rekisterinpitäjän/henkilötietojen käsittelijän osalta, ja heillä olisi oltava mahdollisuus poistaa kyseiset tiedot ottaen huomioon tietojenkäsittelyn tarkoitus ja oikeusperuste;
- tietoja ei pitäisi siirtää kolmansille osapuolille (eli ainoastaan käyttäjällä on pääsy tietoihin);
- tietoja olisi säilytettävä vain niin kauan kuin on tarpeen palvelun tarjoamiseksi tai niin kauan kuin unionin tai jäsenvaltion lainsäädännössä muutoin edellytetään;
- rekisteröityjen olisi voitava poistaa pysyvästi kaikki henkilötiedot ennen ajoneuvon myyntiä;
- rekisteröidyillä olisi mahdollisuuksien mukaan oltava suora pääsy näiden sovellusten tuottamiin tietoihin.

78. Vaikka paikallinen tietojenkäsittely ei aina ole mahdollista kussakin käyttötapauksessa, ns. yhdistelmäkäsittelyä voidaan kuitenkin usein hyödyntää. Esimerkiksi käyttöön perustuvan vakuutuksen yhteydessä ajokäyttäytymistä koskevia henkilötietoja (kuten jarrupolkimeen kohdistuva voima, ajettu kilometrimäärä jne.) voitaisiin käsitellä joko ajoneuvon sisällä, tai niitä voi käsitellä telemaattisten palvelujen tarjoaja vakuutusyhtiön (rekisterinpitäjä) puolesta siten, että vakuutusyhtiölle annetaan numeeriset pisteet sovitulla tavalla (esim. kuukausittain). Tällä tavoin vakuutusyhtiö ei saa käyttöönsä käyttäytymistä koskevia raakatietoja vaan ainoastaan käsittelyn tuloksena saadun kokonaispistemäärän. Näin varmistetaan, että tietojen minimoinnin periaatteita noudatetaan sisäänrakennetusti. Tämä tarkoittaa myös sitä, että käyttäjillä on oltava mahdollisuus käyttää oikeuksiaan, kun muut osapuolet tallentavat tietoja: käyttäjän olisi esimerkiksi voitava poistaa autokorjaamon tai jälleenmyyjän järjestelmiin tallennetut tiedot yleisen tietosuoja-asetuksen 17 artiklan mukaisesti.

[40] Katso sisäänrakennettua ja oletusarvoista yksityisyyden suojaa koskevia suosituksia ohjeista 4/2019.
[41] Tietosuojatyöryhmän lausunto 5/2012 tietotekniikan resurssipalveluista; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_fi.pdf

2.4.2 Anonymisointi ja pseudonymisointi

79. Jos henkilötietoja aiotaan siirtää ajoneuvon ulkopuolelle, olisi harkittava niiden anonymisointia ennen niiden siirtämistä. Rekisterinpitäjän olisi otettava anonymisoinnissa huomioon kaikki asiaan liittyvä käsittely, joka saattaa johtaa tietojen uudelleentunnistamiseen, kuten paikallisesti anonymisoitujen tietojen siirtäminen. Euroopan tietosuojaneuvosto muistuttaa, että tietosuojaperiaatteita ei sovelleta anonyymeihin tietoihin eli tietoihin, jotka eivät liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, tai henkilötietoihin, joiden tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole tai ei ole enää mahdollista.[42] Sen jälkeen, kun tietoaineisto on tosiasiassa anonymisoitu eikä yksilöitä voida enää tunnistaa, EU:n tietosuojalainsäädäntöä ei enää sovelleta. Anonymisointi voi olla hyvä strategia, jolla verkkoon liitettyjen ajoneuvojen hyödyt säilytetään ja riskejä lievennetään.

80. Kuten 29 artiklan mukaisen tietosuojatyöryhmän anonymisointitekniikkoja koskevassa lausunnossa[43] todetaan, tietojen anonymisointiin voidaan käyttää erilaisia menetelmiä ja joskus niiden yhdistelmää.

81. Muut tekniikat, kuten pseudonymisointi[44], voivat auttaa minimoimaan tietojen käsittelystä aiheutuvat riskit, kun otetaan huomioon, että useimmissa tapauksissa suoraan tunnistettavat tiedot eivät ole tarpeen käsittelyn tarkoituksen saavuttamiseksi. Pseudonymisointi vähentää väärinkäytön riskiä ja näin parantaa henkilötietojen suojaa, jos sitä vahvistetaan suojatoimilla. Toisin kuin anonymisointi, pseudonymisointi voidaan kumota, ja pseudonymisoituja tietoja pidetään yleisen tietosuoja-asetuksen soveltamisalaan kuuluvina henkilötietoina.

2.4.3 Tietosuojaa koskeva vaikutustenarviointi

82. Kun otetaan huomioon verkkoon liitettyjen ajoneuvojen avulla tuotettavien henkilötietojen laajuus ja arkaluonteisuus, on todennäköistä, että käsittely – erityisesti tilanteissa, joissa henkilötietoja käsitellään ajoneuvon ulkopuolella – aiheuttaa usein suuren riskin yksilöiden oikeuksille ja vapauksille. Tällaisessa tapauksessa alan toimijoiden on toteutettava riskien tunnistamiseksi ja lieventämiseksi tietosuojaa koskeva vaikutustenarviointi yleisen tietosuoja-asetuksen 35 ja 36 artiklan mukaisesti. Jopa tapauksissa, joissa tietosuojaa koskevaa vaikutustenarviointia ei vaadita, parhaana käytäntönä on tehdä se mahdollisimman varhaisessa vaiheessa suunnitteluprosessia. Alan toimijat voivat ottaa tämän analyysin tulokset huomioon suunnitteluvalinnoissaan ennen uusien teknologioiden käyttöönottoa.

2.5 Tiedot

83. Ennen henkilötietojen käsittelyä rekisteröidylle on ilmoitettava rekisterinpitäjän identiteetti (esim. ajoneuvon ja laitteen valmistaja tai palveluntarjoaja), käsittelyn tarkoitus, tietojen

[42] Ks. yleisen tietosuoja-asetuksen 4 artiklan 1 kohta ja johdanto-osan 26 kappale.
[43] Tietosuojatyöryhmän lausunto 5/2014 anonymisointitekniikoista; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf
[44] Yleisen tietosuoja-asetuksen 4 artiklan 5 kohta. ENISAn raportti, 3. joulukuuta 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

vastaanottajat, tietojen säilytysaika ja rekisteröidyn yleisen tietosuoja-asetuksen mukaiset oikeudet.[45]

84. Lisäksi ajoneuvon ja laitteiden valmistajan, palveluntarjoajan tai muun rekisterinpitäjän olisi annettava rekisteröidylle seuraavat selkeät, yksinkertaiset ja helposti saatavilla olevat tiedot:

- tietosuojavastaavan yhteystiedot;
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;
- nimenomainen maininta rekisterinpitäjän tai kolmannen osapuolen oikeutetuista eduista, jos ne muodostavat käsittelyn oikeusperusteen;
- mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät;
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;
- rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;
- rekisteröidyn oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu suostumukseen;
- tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tietojen siirtämisessä käytetyistä suojatoimista;
- onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;
- automaattisen päätöksenteon, muun muassa profiloinnin, jolla on rekisteröityä koskevia oikeusvaikutuksia tai joka vaikuttaa rekisteröityyn vastaavalla tavalla merkittävästi, olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle. Tämä voi koskea erityisesti käyttöön perustuvan vakuutuksen tarjoamista yksityishenkilöille;
- oikeus tehdä valitus valvontaviranomaiselle;
- tiedot myöhemmästä käsittelystä;
- yhteisrekisterinpitäjien tapauksessa selkeät ja täydelliset tiedot kunkin rekisterinpitäjän vastuualueista.

85. Joissakin tapauksissa henkilötietoja ei kerätä suoraan asianomaiselta henkilöltä. Ajoneuvojen ja laitteiden valmistaja voi esimerkiksi luottaa siihen, että jälleenmyyjä kerää ajoneuvon omistajaa koskevia tietoja tarjotakseen tienvarsipalveluja hätätilanteissa. Jos

[45] Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan a alakohta ja 13 artikla. Ks. myös tietosuojatyöryhmän asetuksen (EU) 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat (wp260rev.01) (Euroopan tietosuojaneuvoston vahvistama asiakirja).

tietoja ei ole kerätty suoraan, ajoneuvon ja laitteen valmistajan, palveluntarjoajan tai muun rekisterinpitäjän on edellä mainittujen tietojen lisäksi ilmoitettava myös kyseessä olevat henkilötietoryhmät, lähde, josta henkilötiedot ovat peräisin, ja tarvittaessa se, ovatko kyseiset tiedot peräisin julkisista lähteistä. Rekisterinpitäjän on toimitettava nämä tiedot kohtuullisen ajan kuluessa tietojen saamisesta ja tietosuoja-asetuksen 14 artiklan 3 kohdan mukaisesti **viimeistään ensimmäisenä seuraavista päivämääristä**: i) kuukauden kuluessa henkilötietojen saamisesta ottaen huomioon tietojen käsittelyyn liittyvät erityiset olosuhteet, ii) kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran, tai iii) jos henkilötiedot siirretään kolmannelle osapuolelle, ennen tietojen toimittamista.

86. Uusia tietoja voi olla tarpeen antaa rekisteröidyille myös, kun niistä vastaa uusi rekisterinpitäjä. Eri rekisterinpitäjät voivat tarjota tienvarsipalvelua, joka on vuorovaikutuksessa verkkoon liitettyjen ajoneuvojen kanssa, riippuen siitä, missä maassa tai millä alueella apua tarvitaan. Uusien rekisterinpitäjien olisi annettava rekisteröidyille vaaditut tiedot, kun rekisteröidyt ylittävät rajan ja kun uudet rekisterinpitäjät tarjoavat palveluja, jotka ovat vuorovaikutuksessa verkkoon liitettyjen ajoneuvojen kanssa.

87. Rekisteröidyille tarkoitetut tiedot voidaan antaa eri tasoissa[46] eli siten, että tiedot erotetaan kahdelle tasolle: yhtäältä ensimmäisen tason tiedot, jotka ovat rekisteröityjen kannalta tärkeimpiä, ja toisaalta tiedot, joiden voidaan olettaa olevan merkityksellisiä myöhemmässä vaiheessa. Ensimmäisen tason olennaisiin tietoihin kuuluvat rekisterinpitäjän identiteetin lisäksi käsittelyn tarkoitus ja kuvaus rekisteröidyn oikeuksista sekä mahdolliset lisätiedot käsittelystä, joka vaikuttaa rekisteröityyn eniten ja joka voi tulla rekisteröidylle yllätyksenä. Euroopan tietosuojaneuvosto suosittelee, että verkkoon liitettyjen ajoneuvojen osalta rekisteröidylle olisi ilmoitettava kaikki ensimmäisen tason tietojen vastaanottajat. Kuten tietosuojatyöryhmän läpinäkyvyyttä koskevissa ohjeissa todetaan, rekisterinpitäjän on annettava vastaanottajista rekisteröityjen kannalta olennaisimmat tiedot. Käytännössä tämä tarkoittaa yleensä nimettyjä vastaanottajia, jotta rekisteröidyt tietävät, millä tahoilla heidän henkilötietojaan on. Jos rekisterinpitäjät eivät pysty ilmoittamaan vastaanottajien nimiä, tiedot tulisi antaa mahdollisimman tarkasti kertomalla vastaanottajan tyyppi (viittaamalla sen harjoittamaan toimintaan), toimiala ja sen alaluokat sekä sijainti.

88. Rekisteröidyille voidaan antaa tiedot tiiviisti esitetyssä ja helposti ymmärrettävässä muodossa ajoneuvon myyntisopimuksessa, palvelusopimuksessa ja/tai millä tahansa kirjallisella välineellä käyttämällä erillisiä asiakirjoja (esim. ajoneuvon huoltokirjanpitoa tai -käsikirjaa) tai kojelautatietokonetta.

89. Yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaisesti tarvittavien tietojen lisäksi voitaisiin käyttää vakiomuotoisia kuvakkeita läpinäkyvyyden lisäämiseksi. Näin voidaan mahdollisesti vähentää tarvetta esittää rekisteröidylle suuri määrä kirjallista tietoa. Niiden olisi oltava näkyvissä ajoneuvoissa, jotta suunnitellusta käsittelystä voidaan antaa hyvä yleiskuva ymmärrettävällä ja selvästi luettavissa olevalla tavalla. Euroopan tietosuojaneuvosto korostaa, että on tärkeää, että kyseiset kuvakkeet ovat vakiomuotoisia, jotta käyttäjä voi löytää samat symbolit ajoneuvon merkistä tai mallista riippumatta. Esimerkiksi tietyntyyppisiä tietoja, kuten sijaintitietoja, kerättäessä ajoneuvossa voisi olla

[46] Ks. tietosuojatyöryhmän asetuksen (EU) 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat (wp260rev.01) (Euroopan tietosuojaneuvoston vahvistama asiakirja).

selkeä merkki (kuten valo ajoneuvon sisällä), joka ilmoittaa matkustajille tietojen keräämisestä.

2.6 Rekisteröidyn oikeudet

90. Ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien olisi helpotettava rekisteröityjen mahdollisuuksia valvoa tietojaan koko käsittelyn ajan ottamalla käyttöön erityisiä välineitä, joilla rekisteröidyt voivat käyttää tehokkaasti oikeuksiaan, erityisesti oikeutta saada pääsy tietoihin, oikaista ja poistaa tiedot, rajoittaa käsittelyä ja käsittelyn oikeusperusteesta riippuen oikeutta siirtää tiedot järjestelmästä toiseen ja vastustaa henkilötietojen käsittelyä.

91. Asetusten muuttamisen helpottamiseksi olisi otettava käyttöön profiilinhallintajärjestelmä, jotta tunnettujen kuljettajien mieltymykset voidaan tallentaa ja jotta kuljettajat voivat muuttaa yksityisyysasetuksiaan helposti milloin tahansa. Profiilinhallintajärjestelmään olisi keskitettävä kaikki tietoasetukset kutakin tietojenkäsittelyä varten, jotta voidaan erityisesti helpottaa henkilötietojen saatavuutta, poistamista ja siirrettävyyttä ajoneuvojärjestelmistä rekisteröidyn pyynnöstä. Kuljettajien olisi voitava milloin tahansa keskeyttää tietyntyyppisten tietojen kerääminen väliaikaisesti tai pysyvästi, ellei ole olemassa erityistä oikeudellista perustetta sille, että rekisterinpitäjä voi jatkaa tiettyjen tietojen keräämistä. Jos kyseessä on sopimus, jossa tarjotaan ajokäyttäytymiseen perustuva henkilökohtainen tarjous, tämä voi merkitä sitä, että käyttäjälle olisi palautettava kyseisen sopimuksen vakioehdot. Nämä ominaisuudet olisi toteutettava ajoneuvon sisällä, mutta niitä voitaisiin tarjota rekisteröidyille myös muilla keinoin (esim. erityisellä sovelluksella). Euroopan tietosuojaneuvosto suosittelee, että valmistajat tarjoavat yksinkertaisen toiminnon (kuten poistopainikkeen), jolla rekisteröidyt voisivat poistaa auton yleisnäkymään tallennettavia henkilötietoja (esim. GPS-navigointihistoria tai selaustiedot) nopeasti ja helposti.

92. Verkkoon liitetyn ajoneuvon myynnin ja siitä johtuvan omistusoikeuden muutoksen olisi myös johdettava sellaisten henkilötietojen poistamiseen, joita ei enää tarvita edellä kuvattuihin erityisiin tarkoituksiin, ja rekisteröidyn olisi voitava käyttää oikeuttaan tietojen siirtoon järjestelmästä toiseen.

2.7 Turvallisuus

93. Ajoneuvojen ja laitteiden valmistajien, palveluntarjoajien ja muiden rekisterinpitäjien olisi otettava käyttöön toimenpiteitä, joilla taataan käsiteltyjen tietojen turvallisuus ja luottamuksellisuus, ja toteutettava kaikki tarvittavat varotoimet estääkseen luvattoman henkilön suorittaman valvonnan. Alan toimijoiden olisi harkittava erityisesti seuraavien toimenpiteiden toteuttamista:

- viestintäkanavien salaus huipputason algoritmin avulla;
- sellaisen salausavainten hallintajärjestelmän käyttöönotto, joka on yksilöllinen kunkin ajoneuvon (ei mallin) osalta;
- kun käytetään etätallennusta, tietojen salaus huipputason algoritmin avulla;
- salausavainten säännöllinen uusiminen;
- salausavainten suojaaminen paljastumiselta;
- tietoja vastaanottavien laitteiden tunnistaminen;

- tietojen eheyden varmistaminen (esim. hajautuksen (*hashing*) avulla);
- luotettavien käyttäjäntunnistustekniikoiden (salasana, sähköinen varmenne jne.) käytön edellyttäminen henkilötietoihin pääsyä varten.

94. Erityisesti ajoneuvojen valmistajille tietosuojaneuvosto suosittelee seuraavien turvatoimien toteuttamista:

- ajoneuvon elintärkeiden toimintojen eristäminen niistä toiminnoista, jotka käyttävät aina televiestintäkapasiteettia (esim. tieto- ja viihdepalvelut);
- tekniset toimenpiteet, joiden avulla ajoneuvojen valmistajat voivat nopeasti korjata turvallisuuteen liittyviä haavoittuvuuksia ajoneuvon koko käyttöiän ajan;
- ajoneuvon elintärkeiden toimintojen osalta erityisesti liikenteeseen tarkoitettujen turvallisten viestintäkeinojen käytön asettaminen mahdollisuuksien mukaan etusijalle;
- sellaisen hälytysjärjestelmän käyttöönotto ajoneuvon järjestelmiin kohdistuvien hyökkäysten varalta, joka toimii myös rajoitetussa tilassa[47];
- ajoneuvon tietojärjestelmän käyttöä koskevien lokitietojen tallentaminen esimerkiksi enintään kuudelta edeltävältä kuukaudelta, jotta mahdollisen hyökkäyksen alkuperä voidaan määrittää, ja lokitietojen tarkastaminen säännöllisesti mahdollisten poikkeamien havaitsemiseksi.

95. Näitä yleisiä suosituksia olisi täydennettävä erityisvaatimuksilla, joissa otetaan huomioon kunkin tietojenkäsittelyn ominaispiirteet ja tarkoitus.

2.8 Henkilötietojen siirtäminen kolmansille osapuolille

96. Periaatteessa ainoastaan rekisterinpitäjällä ja rekisteröidyllä on pääsy verkkoon liitetyn ajoneuvon tuottamiin tietoihin. Rekisterinpitäjä voi kuitenkin siirtää henkilötietoja kaupalliselle kumppanille (vastaanottajalle), jos siirto perustuu lainmukaisesti johonkin yleisen tietosuoja-asetuksen 6 artiklan mukaisista oikeusperusteista.

97. Koska ajoneuvon käyttöä koskevat tiedot (esim. matkat, ajotyyli) voivat olla arkaluonteisia, Euroopan tietosuojaneuvosto suosittelee, että rekisteröidyn suostumus hankitaan systemaattisesti ennen kuin hänen tietonsa toimitetaan rekisterinpitäjänä toimivalle kaupalliselle kumppanille (esim. rastitetaan ruutu, jota ei ole ennalta rastitettu, tai jos se on teknisesti mahdollista, käytetään fyysistä tai loogista välinettä, jota henkilö voi käyttää ajoneuvosta käsin). Kaupallinen kumppani puolestaan vastaa saamistaan tiedoista, ja siihen sovelletaan kaikkia yleisen tietosuoja-asetuksen säännöksiä.

98. Ajoneuvon valmistaja, palveluntarjoaja tai muu rekisterinpitäjä voi siirtää henkilötietoja henkilötietojen käsittelijälle, joka on valittu osallistumaan palvelun tarjoamiseen rekisteröidylle, edellyttäen, että henkilötietojen käsittelijä ei käytä näitä tietoja omaan käyttöönsä. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on laadittava sopimus tai

[47] Rajoitettu tila on ajoneuvon käyttötila, jolla varmistetaan, että ajoneuvon turvallisen toiminnan kannalta olennaiset toiminnot (eli turvallisuutta koskevat vähimmäisvaatimukset) taataan, vaikka muut vähemmän tärkeät toiminnot poistettaisiin käytöstä (esim. navigointilaitteen toiminta voidaan katsoa epäolennaiseksi, toisin kuin jarrujärjestelmä).

muu oikeudellinen asiakirja, jossa täsmennetään kunkin osapuolen velvoitteet ja vahvistetaan yleisen tietosuoja-asetuksen 28 artiklan säännökset.

2.9 Henkilötietojen siirtäminen EU/ETAn ulkopuolelle

99. Kun henkilötietoja siirretään Euroopan talousalueen ulkopuolelle, käytössä on erityisiä suojakeinoja, joilla varmistetaan, että tietosuoja siirtyy tietojen mukana.

100. Näin ollen rekisterinpitäjä voi siirtää henkilötietoja vastaanottajalle vain siltä osin kuin siirto on yleisen tietosuoja-asetuksen V luvussa säädettyjen vaatimusten mukaista.

2.10 Ajoneuvon langattomien tekniikoiden käyttö

101. Matkapuhelinteknologian kehittymisen myötä internetin käytöstä liikenteessä on tullut helppoa. Vaikka ajoneuvoon voidaan saada langaton yhteys älypuhelinten hotspot-tukiaseman tai erityisen laitteen (esim. OBD-II-mokkula, langaton modeemi tai reititin) kautta, useimmat valmistajat tarjoavat nykyisin malleja, joihin sisältyy sisäänrakennettu mobiilidatayhteys ja joilla voidaan myös luoda langattomia verkkoja. Tapauksen mukaan on otettava huomioon eri näkökohtia:

   - Tieliikenteen ammattilainen, kuten taksinkuljettaja, tarjoaa langattoman yhteyden usein palveluna asiakkailleen. Tässä tapauksessa ammattihenkilöä tai hänen yritystään voidaan pitää internetpalvelun tarjoajana, joten siihen sovelletaan asiakkaan henkilötietojen käsittelyä koskevia erityisiä velvoitteita ja rajoituksia.

   - Langaton yhteys on tarkoitettu ainoastaan kuljettajan (ei sekä kuljettajan että matkustajien) käyttöä varten. Tässä tapauksessa henkilötietojen käsittely katsotaan yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan c alakohdassa ja johdanto-osan 18 kappaleessa tarkoitetuksi yksinomaan henkilökohtaiseksi tai kotitaloutta koskevaksi toiminnaksi.

102. Langattomien internetyhteyksien käyttöliittymien yleistyminen lisää yleensä yksilöiden yksityisyyteen kohdistuvia riskejä. Käyttäjät lähettävät ajoneuvojensa kautta jatkuvasti tietoja, ja tämän vuoksi käyttäjät voidaan tunnistaa ja jäljittää. Jäljittämisen estämiseksi ajoneuvojen ja laitteiden valmistajien olisi otettava käyttöön helppokäyttöisiä valintamahdollisuuksia, joilla varmistetaan, että ajoneuvon langattoman verkon verkkotunnusta (SSID) ei kerätä.

3 ESIMERKKITAPAUKSET

103. Tässä kohdassa käsitellään viittä esimerkkiä tietojenkäsittelystä verkkoon liitetyissä ajoneuvoissa. Esimerkit vastaavat skenaarioita, joita alan sidosryhmille todennäköisesti tulee vastaan. Esimerkkejä ovat tietojenkäsittely, joka edellyttää laskentatehoa, jota ei voida ottaa käyttöön paikallisesti ajoneuvossa, ja/tai henkilötietojen lähettämistä kolmannelle osapuolelle lisäanalyysien tekemiseksi tai toimintojen lisäämiseksi etäyhteyden välityksellä. Tässä asiakirjassa eritellään kunkin käsittelytyypin osalta suunnitellut tarkoitukset, kerättyjen tietojen ryhmät, tietojen säilytysaika, rekisteröityjen oikeudet, toteutettavat turvatoimet ja tietojen vastaanottajat. Jos joitakin näistä seikoista ei ole kuvattu jäljempänä, sovelletaan edellisessä osassa kuvattuja yleisiä suosituksia.

104. Valitut esimerkit eivät ole tyhjentäviä, vaan niillä on tarkoitus osoittaa, minkä tyyppistä käsittelyä ja minkä tyyppisiä oikeusperusteita, toimijoita jne. verkkoon liitettyihin ajoneuvoihin voi liittyä.

3.1 Kolmannen osapuolen tarjoama palvelu

105. Rekisteröidyt voivat tehdä sopimuksen palveluntarjoajan kanssa saadakseen ajoneuvoonsa liittyviä lisäarvopalveluja. Rekisteröity voi esimerkiksi tehdä käyttöön perustuvan vakuutussopimuksen, jossa tarjotaan alennettuja vakuutusmaksuja vähemmästä ajamisesta (”Pay As You Drive”) tai hyvästä ajokäyttäytymisestä (”Pay How You Drive”) ja joka edellyttää, että vakuutusyhtiö seuraa ajotottumuksia. Rekisteröity voi myös tehdä sopimuksen sellaisen yrityksen kanssa, joka tarjoaa tienvarsiapua vian sattuessa. Sopimukseen liittyy ajoneuvon sijainnin siirtämistä yritykselle tai palveluntarjoajalle

ajoneuvon toimintaa koskevien viestien tai varoitusten vastaanottamiseksi (esim. varoitus jarrujen kulumisesta tai muistutus katsastuspäivästä).

3.1.1 Käyttöön perustuvat vakuutukset

106. ”Pay as you drive” -vakuutuksella tarkoitetaan käyttöön perustuvaa vakuutusta, jossa seurataan kuljettajan ajokilometrien määrää ja/tai ajotottumuksia, jotta voidaan yksilöidä turvalliset kuljettajat ja palkita heidät tarjoamalla heille alhaisempia vakuutusmaksuja. Vakuutuksenantaja edellyttää, että kuljettaja asentaa sisäänrakennetun telemaattisen palvelun tai mobiilisovelluksen tai aktivoi valmistajalta saadun sisäänrakennetun moduulin, joka seuraa vakuutuksenottajan ajamia kilometrejä ja/tai ajokäyttäytymistä (esim. jarrutustapa tai nopea kiihdyttäminen). Telemaattisella laitteella kerättyjen tietojen perusteella määritetään kuljettajan pistemäärä, jotta voidaan analysoida riskejä, joita hän voi aiheuttaa vakuutusyhtiölle.

107. Koska käyttöön perustuva vakuutus edellyttää sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaista suostumusta, Euroopan tietosuojaneuvosto toteaa, että vakuutuksenottajalla on oltava mahdollisuus valita muu kuin käyttöön perustuva vakuutus. Muussa tapauksessa suostumusta ei voitaisi pitää vapaaehtoisesti annettuna, koska sopimuksen täytäntöönpano edellyttäisi suostumusta. Lisäksi yleisen tietosuoja-asetuksen 7 artiklan 3 kohdassa edellytetään, että rekisteröidyllä on oltava oikeus peruuttaa suostumuksensa.

3.1.1.1 Oikeusperuste

108. Kun tiedot kerätään yleisesti saatavilla olevan sähköisen viestintäpalvelun kautta (esimerkiksi telemaattiseen laitteeseen sisältyvän SIM-kortin kautta), ajoneuvoon tallennettujen tietojen käyttämiseen tarvitaan suostumus sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaisesti. Mitään kyseisissä säännöksissä säädetyistä poikkeuksista ei voida soveltaa tässä yhteydessä: käsittelyn ainoana tarkoituksena ei ole viestinnän välittäminen sähköisissä viestintäverkoissa, eikä se liity tilaajan tai käyttäjän erityisesti pyytämään tietoyhteiskuntapalveluun. Suostumus voitaisiin kerätä sopimuksenteon hetkellä.

109. Mitä tulee henkilötietojen käsittelyyn tallentamisen jälkeen tai loppukäyttäjän päätelaitteen käyttöön, vakuutusyhtiö voi tässä yhteydessä vedota yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohtaan edellyttäen, että se voi osoittaa, että käsittely tapahtuu rekisteröidyn kanssa tehdyn voimassa olevan sopimuksen puitteissa ja että käsittely on tarpeen rekisteröidyn kanssa tehdyn sopimuksen täytäntöön panemiseksi. Jos käsittely on objektiivisesti katsoen tarpeen rekisteröidyn kanssa tehdyn sopimuksen täytäntöön panemiseksi, Euroopan tietosuojaneuvosto katsoo, että yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohtaan vetoaminen ei heikentäisi tässä nimenomaisessa tapauksessa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädettyä lisäsuojaa. Tämä oikeusperuste toteutuu siten, että rekisteröity allekirjoittaa sopimuksen vakuutusyhtiön kanssa.

3.1.1.2 Kerätyt tiedot

110. Huomioon otettavia henkilötietoja on kahdenlaisia:

- **kaupalliset ja liiketapahtumaan liittyvät tiedot**: esim. rekisteröidyn tunnistetiedot, liiketapahtumaan liittyvät tiedot ja maksuvälineitä koskevat tiedot;

- **käyttötiedot**: esim. ajoneuvon tuottamat henkilötiedot, ajotottumukset ja sijaintitiedot.

111. Euroopan tietosuojaneuvosto suosittelee, että koska on olemassa vaara, että telemaattisen yksikön kautta kerättyjä tietoja voidaan käyttää väärin tarkan profiilin luomiseksi kuljettajan liikkeistä, ajokäyttäytymistä koskevia raakatietoja olisi mahdollisuuksien mukaan käsiteltävä seuraavasti:

- ajoneuvon sisällä telemaattisissa yksiköissä tai käyttäjän älypuhelimessa siten, että vakuutuksenantaja saa käyttöönsä ainoastaan tulostiedot (esim. ajotottumuksiin liittyvän pistemäärän), ei yksityiskohtaisia raakatietoja (ks. kohta 2.1);

- tai rekisterinpitäjän (vakuutusyhtiö) puolesta toimiva telemaattisten palvelujen tarjoaja tuottaa numeeriset pistemäärät, jotka siirretään vakuutusyhtiölle määritetyllä tavalla. Tällöin raakatiedot ja tiedot, jotka liittyvät suoraan kuljettajan henkilöllisyyteen, on erotettava toisistaan. Tämä tarkoittaa sitä, että telemaattisten palvelujen tarjoaja saa reaaliaikaiset tiedot, mutta ei tietoa esimerkiksi vakuutuksenottajan nimestä tai rekisterikilvestä. Vakuutuksenottajan nimi on toisaalta vakuutuksenantajan tiedossa, mutta tämä saa tietoonsa ainoastaan pistemäärät ja kokonaiskilometrit, ei näiden pistemäärien tuottamiseen käytettyjä raakatietoja.

112. Lisäksi on huomattava, että jos sopimuksen täyttäminen edellyttää ainoastaan kilometrimäärää, sijaintitietoja ei kerätä.

3.1.1.3 Säilytysaika

113. Sopimuksen täytäntöönpanoon (eli palvelun suorittamiseen) liittyvässä tietojen käsittelyssä on tärkeää erottaa toisistaan kaksi tietotyyppiä ennen kuin niiden säilytysajat voidaan määrittää:

- **kaupalliset ja liiketapahtumaan liittyvät tiedot:** näitä tietoja voidaan säilyttää aktiivisessa tietokannassa sopimuksen koko keston ajan. Sopimuksen päättyessä ne voidaan arkistoida fyysisesti (erilliselle välineelle, kuten DVD:lle) tai loogisesti (valtuutuksien hallinnalla) mahdollisten riita-asioiden yhteydessä. Tämän jälkeen tiedot on poistettava tai anonymisoitava lakisääteisen aikarajan umpeuduttua;

- **käyttötiedot:** käyttötiedot voidaan luokitella raakatiedoiksi ja yhdistelmätiedoiksi. Kuten edellä todettiin, rekisterinpitäjien tai henkilötietojen käsittelijöiden ei mahdollisuuksien mukaan pitäisi käsitellä raakatietoja. Jos raakatietoja tarvitaan, niitä olisi säilytettävä vain niin kauan kuin niitä tarvitaan yhdistelmätietojen laatimiseksi ja yhdistämisprosessin asianmukaisuuden tarkistamiseksi. Yhdistelmätietoja olisi säilytettävä vain niin kauan kuin on tarpeen palvelun tarjoamiseksi tai niin kauan kuin unionin tai jäsenvaltion lainsäädännössä muutoin edellytetään.

3.1.1.4 Tietojen antaminen ja rekisteröityjen oikeudet

114. Rekisteröidylle on ennen henkilötietojen käsittelyä ilmoitettava asiasta yleisen tietosuoja-asetuksen 13 artiklan mukaisesti läpinäkyvällä ja ymmärrettävällä tavalla. Erityisesti rekisteröidylle on ilmoitettava henkilötietojen säilytysaika tai, jos se ei ole mahdollista, tämän ajan määrittämiskriteerit. Euroopan tietosuojaneuvosto suosittelee, että viimeksi mainitussa tapauksessa sovelletaan pedagogista lähestymistapaa, jossa korostetaan raakatietojen ja niiden perusteella saadun pistemäärän välistä eroa ja painotetaan tarvittaessa, että vakuutuksenantaja käyttää pistemäärätulosta vain tarvittaessa.

115. Jos tietoja ei käsitellä ajoneuvossa vaan niitä käsittelee rekisterinpitäjän (vakuutusyhtiön) puolesta toimiva telemaattisten palvelujen tarjoaja, tiedoissa voitaisiin mainita, että tässä

tapauksessa palveluntarjoajalla ei ole pääsyä tietoihin, jotka liittyvät suoraan kuljettajan henkilöllisyyteen (kuten nimi tai rekisterikilpi). Kun otetaan huomioon, että rekisteröidyille on tärkeää tiedottaa heidän henkilötietojensa käsittelyn seurauksista ja että rekisteröidyt eivät saisi yllättyä heidän henkilötietojensa käsittelystä, Euroopan tietosuojaneuvosto suosittelee myös, että rekisteröidylle tiedotetaan profiloinnin olemassaolosta ja sen seurauksista, vaikka siihen ei liittyisi yleisen tietosuoja-asetuksen 22 artiklassa tarkoitettua automaattista päätöksentekoa.

116. Rekisteröidyille on erityisesti ilmoitettava hänen käytettävissään olevista keinoista käyttää oikeutta päästä tietoihin sekä oikaista, rajoittaa ja poistaa tietoja. Koska tässä yhteydessä kerätyt raakatiedot antaa rekisteröity (tätä varten tarkoitetuissa lomakkeissa tai toimintansa myötä) ja niitä käsitellään yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan (sopimuksen täytäntöönpano) perusteella, rekisteröidyllä on oikeus käyttää oikeuttaan tietojen siirtämiseen järjestelmästä toiseen. Euroopan tietosuojaneuvosto suosittelee painokkaasti, kuten oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevissa ohjeissa[48] korostetaan, että ”rekisterinpitäjät selittävät selvästi niiden tietojen välisen eron, jotka rekisteröity voi saada tietoon pääsyä ja tietojen siirtämistä koskevien oikeuksien perusteella”.

117. Tiedot voidaan antaa, kun sopimus allekirjoitetaan.

3.1.1.5 Vastaanottaja:

118. Euroopan tietosuojaneuvosto suosittelee, että ajoneuvon käyttöä koskevat tiedot käsitellään mahdollisuuksien mukaan suoraan telemaattisissa yksiköissä, jotta vakuutuksenantaja saa yksityiskohtaisten raakatietojen sijaan käyttöönsä ainoastaan tulostiedot (esim. pistemäärän).

119. Jos telemaattisten palvelujen tarjoaja kerää tiedot rekisterinpitäjän (vakuutusyhtiön) puolesta numeeristen pisteiden muodostamiseksi, sen ei tarvitse tietää vakuutuksen ottaneen kuljettajan henkilöllisyyttä (kuten nimeä tai rekisterikilpeä).

3.1.1.6 Turvallisuus:

120. Yleisiä suosituksia sovelletaan. Ks. kohta 2.7.

3.1.2 Pysäköintipaikan vuokraaminen ja varaaminen

121. Pysäköintipaikan omistaja saattaa haluta antaa paikan vuokralle. Tätä varten hän ilmoittaa paikasta ja määrittää sen hinnan verkkosovelluksessa. Kun pysäköintipaikasta on ilmoitettu, sovellus ilmoittaa omistajalle, jos kuljettaja haluaa varata sen. Kuljettaja voi valita määränpään ja tarkistaa käytettävissä olevat pysäköintipaikat useiden kriteerien perusteella. Omistajan hyväksynnän jälkeen maksutapahtuma vahvistetaan, ja palveluntarjoaja käsittelee maksutapahtuman ja ohjaa navigoinnin avulla kohteeseen.

3.1.2.1 Oikeusperuste

122. Kun tiedot kerätään yleisesti saatavilla olevan sähköisen viestintäpalvelun kautta, sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa.

[48] Tietosuojatyöryhmän asetuksen 2016/679 mukaista oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet (WP242 rev.01) (Euroopan tietosuojaneuvoston vahvistama asiakirja), s. 13.

123. Koska kyseessä on tietoyhteiskuntapalvelu, sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa ei edellytetä suostumusta ajoneuvoon tallennettujen tietojen käyttöön, kun tilaaja erityisesti pyytää tällaista palvelua.

124. Henkilötietojen käsittelyssä ja ainoastaan kyseisen sopimuksen, jossa rekisteröity on osapuolena, täytäntöönpanon edellyttämien tietojen osalta oikeusperusteena on yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta.

3.1.2.2 Kerätyt tiedot

125. Käsiteltäviin tietoihin sisältyvät kuljettajan yhteystiedot (nimi, sähköpostiosoite, puhelinnumero, ajoneuvotyyppi (esim. henkilöauto, kuorma-auto, moottoripyörä), rekisterinumero, pysäköintiaika, maksutiedot (esim. luottokorttitiedot) ja navigointitiedot.

3.1.2.3 Säilytysaika

126. Tietoja olisi säilytettävä vain niin kauan kuin se on tarpeen pysäköintisopimuksen täyttämiseksi tai kuin unionin tai jäsenvaltion lainsäädännössä muutoin edellytetään. Tämän jälkeen tiedot joko anonymisoidaan tai poistetaan.

3.1.2.4 Tietojen antaminen ja rekisteröityjen oikeudet

127. Rekisteröidylle olisi ennen henkilötietojen käsittelyä ilmoitettava asiasta yleisen tietosuoja-asetuksen 13 artiklan mukaisesti läpinäkyvällä ja ymmärrettävällä tavalla.

128. Rekisteröidyille on erityisesti ilmoitettava hänen käytettävissään olevista keinoista käyttää oikeutta päästä tietoihin sekä oikaista, rajoittaa ja poistaa tietoja. Koska tässä yhteydessä kerätyt tiedot antaa rekisteröity (tätä varten tarkoitetuissa lomakkeissa tai toimintansa myötä) ja niitä käsitellään yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan (sopimuksen täytäntöönpano) perusteella, rekisteröidyllä on oikeus käyttää oikeuttaan tietojen siirtämiseen järjestelmästä toiseen. Euroopan tietosuojaneuvosto suosittelee painokkaasti, kuten oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevissa ohjeissa korostetaan, että ”*rekisterinpitäjät selittävät selvästi niiden tietojen välisen eron, jotka rekisteröity voi saada tietoon pääsyä ja tietojen siirtämistä koskevien oikeuksien perusteella*”.

3.1.2.5 Vastaanottaja:

129. Periaatteessa ainoastaan rekisterinpitäjällä ja henkilötietojen käsittelijällä on pääsy tietoihin.

3.1.2.6 Turvallisuus:

130. Yleisiä suosituksia sovelletaan. Ks. kohta 2.7.

3.2 eCall-palvelu

131. Jos Euroopan unionissa tapahtuu vakava onnettomuus, ajoneuvo käynnistää automaattisesti eCall-puhelun EU:n laajuiseen hätänumeroon 112 (katso lisätietoja kohdasta 1.1), jolloin onnettomuuspaikalle voidaan lähettää ambulanssi viipymättä, hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän käyttöönottoa koskevista tyyppihyväksyntävaatimuksista ja direktiivin 2007/46/EY muuttamisesta 29. huhtikuuta 2015 annetun asetuksen (EU) 2015/758, jäljempänä ’asetus (EU) 2015/758’, mukaisesti.

132. Ajoneuvoon asennettu eCall-yksikkö, joka mahdollistaa tiedonsiirron yleisen langattoman matkaviestinverkon kautta, käynnistää hätäpuhelun, joka aktivoituu joko automaattisesti ajoneuvoon asennettujen antureiden kautta tai jonka ajoneuvon matkustajat aktivoivat

manuaalisesti vain onnettomuuden sattuessa. Äänikanavan aktivoinnin lisäksi onnettomuus aktivoi automaattisesti vähimmäistietojen tuottamisen ja lähettämisen hätäkeskukseen.

3.2.1 Oikeusperuste

133. Sovellettaessa sähköisen viestinnän tietosuojadirektiiviä on otettava huomioon kaksi säännöstä:

- 9 artikla, joka koskee muita paikkatietoja kuin liikennetietoja ja jota sovelletaan ainoastaan sähköisiin viestintäpalveluihin;
- 5 artiklan 3 kohta, kun kyse on ajoneuvoon asennettuun yksikköön tallennettujen tietojen käyttämisestä.

134. Vaikka nämä säännökset edellyttävät periaatteessa rekisteröidyn suostumusta, asetus (EU) 2015/758 muodostaa rekisterinpitäjään sovellettavan oikeudellisen velvoitteen (rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta eikä hän voi kieltää tietojensa käsittelyä). Näin ollen asetus (EU) 2015/758 on etusijalla suhteessa tarpeeseen saada kuljettajan suostumus paikkatietojen ja vähimmäistietojen käsittelyyn.[49]

135. Näiden tietojen käsittelyn oikeusperusteena on yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdassa säädetyn oikeudellisen velvoitteen (eli asetuksen (EU) 2015/758) noudattaminen.

3.2.2 Kerätyt tiedot

136. Asetuksessa (EU) 2015/578 säädetään, että hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän lähettämiin tietoihin on sisällyttävä ainoastaan standardissa EN 15722:2015 (Intelligent transport systems – eSafety – eCall minimum set of data (MSD)) tarkoitetut vähimmäistiedot, joihin kuuluu

- tieto siitä, onko eCall-puhelun aktivoitu manuaalisesti vai automaattisesti;
- ajoneuvon tyyppi;
- ajoneuvon valmistenumero (VIN);
- ajoneuvon käyttövoimatyyppi;
- aikaleima ajankohdasta, jona alkuperäinen tietoviesti tuotettiin kyseisestä eCall-tapahtumasta;
- ajoneuvon sijainnin viimeinen tiedossa oleva leveys- ja pituusaste, joka on määritetty mahdollisimman vähän aikaa ennen viestin tuottamista;
- ajoneuvon viimeinen tiedossa oleva todellinen kulkusuunta, joka on määritetty mahdollisimman vähän aikaa ennen viestin tuottamista (ainoastaan ajoneuvon kolme viimeistä sijaintipaikkaa).

[49] On huomattava, että sähköisen viestinnän tietosuoja-asetusta koskevan neuvoston neuvotteluvaltuutuksen 8 artiklan 1 kohdan f alakohdassa säädetään eCall-järjestelmää koskevasta erityisestä poikkeuksesta, jonka mukaan suostumusta ei tarvita, kun käsittely on tarpeen päätelaitteen paikantamiseksi, kun loppukäyttäjä toteuttaa hätäpuhelun joko eurooppalaiseen hätänumeroon 112 tai kansalliseen hätänumeroon 13 artiklan 3 kohdan mukaisesti.

3.2.3 Säilytysaika

137. Asetuksessa (EU) 2015/758 säädetään, että tietoja ei saa säilyttää pidempään kuin on tarpeen hätätilanteiden käsittelemiseksi. Nämä tiedot on poistettava kokonaan, kun niitä ei enää tarvita tähän tarkoitukseen. Lisäksi eCall-järjestelmän sisäisessä muistissa olevia tietoja on poistettava automaattisesti ja jatkuvasti. Ainoastaan ajoneuvon kolme viimeistä sijaintipaikkaa voidaan säilyttää siltä osin kuin se on ehdoton edellytys senhetkisen sijainnin ja sen suunnan määrittämiselle, johon oltiin matkalla tapahtuman aikana.

3.2.4 Tietojen antaminen ja rekisteröityjen oikeudet

138. Asetuksen (EU) 2015/758 6 artiklassa säädetään, että valmistajien on annettava selkeät ja perusteelliset tiedot eCall-järjestelmän kautta tapahtuvasta tietojen käsittelystä. Nämä tiedot on annettava omistajan käsikirjassa erikseen hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän ja mahdollisen kolmannen osapuolen palvelujen tukeman eCall-järjestelmän osalta ennen järjestelmän käyttöä. Tietoihin kuuluu muun muassa

- viittaus käsittelyn oikeusperusteeseen;
- tieto siitä, että hätänumeroon 112 perustuva ajoneuvoon asennettava eCall-järjestelmä on oletusarvoisesti toiminnassa;
- yksityiskohtaiset tiedot hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän toteuttamasta tietojen käsittelystä;
- eCall-järjestelmän kautta tapahtuvan tietojenkäsittelyn erityinen tarkoitus, joka on rajattava asetuksen (EU) 2015/758 5 artiklan 2 kohdan ensimmäisessä alakohdassa tarkoitettuihin hätätilanteisiin;
- kerättävien ja käsiteltävien tietojen tyypit sekä näiden tietojen vastaanottajat;
- aikaraja tietojen säilyttämiselle hätänumeroon 112 perustuvassa ajoneuvoon asennettavassa eCall-järjestelmässä;
- ilmoitus siitä, että ajoneuvoon ei kohdistu jatkuvaa paikannusta;
- yksityiskohtaiset tiedot siitä, miten rekisteröidyt henkilöt voivat käyttää oikeuksiaan, sekä tiedonsaantipyyntöjen käsittelystä vastaavasta yhteyspalvelusta;
- kaikki tarvittavat lisätiedot, jotka koskevat henkilötietojen jäljitettävyyttä, paikantamista ja käsittelyä kolmannen osapuolen palvelujen tukeman eCall-palvelun ja/tai muun lisäarvopalvelun tarjoamisen yhteydessä; tällöin edellytetään omistajan nimenomaista suostumusta ja yleisen tietosuoja-asetuksen noudattamista. Erityistä huomiota on kiinnitettävä eroihin, joita saattaa esiintyä hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän ja kolmannen osapuolen palvelujen tukemien ajoneuvoon asennettavien eCall-järjestelmien tai muiden lisäarvopalvelujen kautta tapahtuvan tietojen käsittelyn välillä.

139. Lisäksi palveluntarjoajan on yleisen tietosuoja-asetuksen 13 artiklan mukaisesti annettava rekisteröidyille tietoja läpinäkyvällä ja ymmärrettävällä tavalla. Rekisteröidylle on erityisesti ilmoitettava henkilötietojen käsittelyn tarkoitukset sekä tieto siitä, että henkilötietojen käsittely perustuu rekisterinpitäjään sovellettavaan oikeudelliseen velvoitteeseen.

140. Lisäksi käsittelyn luonne huomioon ottaen henkilötietojen vastaanottajia tai vastaanottajaryhmiä koskevien tietojen olisi oltava selkeitä, ja rekisteröidyille olisi ilmoitettava, että tiedot eivät ole hätänumeroon 112 perustuvan ajoneuvoon asennettavan järjestelmän ulkopuolisen tahon käytettävissä ennen kuin eCall-puhelu on aloitettu.

141. Rekisteröityjen oikeuksien osalta on huomattava, että koska käsittely perustuu oikeudelliseen velvoitteeseen, oikeutta vastustaa käsittelyä ja oikeutta tietojen siirtoon ei sovelleta.

3.2.5 Vastaanottaja:

142. Tiedot eivät saa olla hätänumeroon 112 perustuvan ajoneuvoon asennettavan järjestelmän ulkopuolisen tahon käytettävissä ennen kuin eCall-puhelu on aloitettu.

143. Kun puhelu aloitetaan (ajoneuvon matkustajat aloittavat sen manuaalisesti tai se käynnistetään automaattisesti heti, kun ajoneuvoon asennettu anturi havaitsee vakavan törmäyksen), eCall-järjestelmä luo puheyhteyden asianomaiseen hätäkeskukseen ja vähimmäistiedot lähetetään hätäkeskuksen operaattorille.

144. Hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän kautta välitettyjä ja hätäkeskusten käsittelemiä tietoja voidaan siirtää päätöksessä N:o 585/2014/EU tarkoitetuille hätäpalveluille ja palvelukumppaneille ainoastaan eCall-puheluihin liittyvissä onnettomuustilanteissa ja kyseisessä päätöksessä vahvistetuin edellytyksin ja käyttää yksinomaan kyseisen päätöksen tavoitteiden saavuttamiseksi. Tietoja, joita hätäkeskukset käsittelevät hätänumeroon 112 perustuvan ajoneuvoon asennettavan eCall-järjestelmän kautta, ei saa siirtää muille kolmansille osapuolille ilman rekisteröidyn henkilön ennakolta antamaa nimenomaista suostumusta.

3.2.6 Turvallisuus

145. Asetuksessa (EU) 2015/758 vahvistetaan vaatimukset, jotka koskevat yksityisyyttä tukevan tekniikan sisällyttämistä eCall-järjestelmään, jotta käyttäjät saavat asianmukaisen tasoisen yksityisyyden suojan, sekä tarvittavia suojatoimia tarkkailun ja väärinkäytön estämiseksi. Lisäksi valmistajien olisi varmistettava, että hätänumeroon 112 perustuva eCall-järjestelmä sekä kaikki muut kolmannen osapuolen palvelujen tukeman eCall-palvelun tai lisäarvopalvelun tuottavat järjestelmät ovat siten suunniteltuja, ettei henkilötietojen vaihtaminen niiden välillä ole mahdollista.

146. Hätäkeskusten osalta jäsenvaltioiden on varmistettava, että henkilötiedot suojataan väärinkäytöksiltä, kuten luvattomalta käytöltä, muokkaamiselta tai häviämiseltä, ja että henkilötietojen tallentamista, säilyttämisen kestoa, käsittelyä ja suojaa koskevat protokollat vahvistetaan asianmukaisella tasolla ja että niitä noudatetaan asianmukaisesti.

3.3 Onnettomuustutkimukset

147. Rekisteröidyt voivat vapaaehtoisesti suostua osallistumaan onnettomuustutkimuksiin, joiden tarkoituksena on ymmärtää paremmin liikenneonnettomuuksien syitä ja jotka on tarkoitettu yleisemmin tieteellisiin tarkoituksiin.

3.3.1 Oikeusperuste

148. Kun tiedot kerätään yleisesti saatavilla olevan viestintäpalvelun kautta, rekisterinpitäjän on sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaisesti hankittava rekisteröidyn suostumus ajoneuvoon tallennettujen tietojen käyttämiseen. Mitään kyseisissä säännöksissä säädetyistä poikkeuksista ei voida soveltaa tässä yhteydessä:

käsittelyn ainoana tarkoituksena ei ole viestinnän välittäminen sähköisissä viestintäverkoissa, eikä se liity tilaajan tai käyttäjän erityisesti pyytämään tietoyhteiskuntapalveluun.

149. Tietosuojaneuvosto suosittelee, että henkilötietojen käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan mukaiseen rekisteröidyn ennalta antamaan suostumukseen, kun otetaan huomioon henkilötietojen moninaisuus ja määrä. Tällainen ennalta annettu suostumus on annettava erityisellä lomakkeella, jolla rekisteröity voi vapaaehtoisesti osallistua tutkimukseen ja varmistaa, että hänen henkilötietojaan käsitellään kyseistä tarkoitusta varten. Suostumuksen on ilmennettävä sen henkilön vapaata, yksilöityä ja tietoista tahtoa, jonka tietoja käsitellään (esim. rastitetaan ruutu, jota ei ole valmiiksi rastitettu, tai määritetään kojelautatietokone toiminnon aktivoimiseksi ajoneuvossa). Tällainen suostumus on annettava erikseen tiettyjä tarkoituksia varten, eikä sitä voi liittää uuden auton osto- tai vuokrasopimukseen. Suostumus on voitava peruuttaa yhtä helposti kuin se annetaan. Suostumuksen peruuttamisen on johdettava käsittelyn lopettamiseen. Tämän jälkeen tiedot poistetaan aktiivisesta tietokannasta tai anonymisoidaan.

150. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa edellytetty suostumus ja tietojen käsittelyn oikeusperusteeksi tarvittava suostumus voidaan kerätä samaan aikaan (esimerkiksi rastitetaan ruutu, josta käy selvästi ilmi, mihin rekisteröity antaa suostumuksensa).

151. On huomattava, että käsittelyn ehdoista riippuen (rekisterinpitäjän luonne jne.) voidaan laillisesti valita toinen oikeusperuste, kunhan se ei heikennä sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädettyä lisäsuojaa (ks. alakohta 15). Jos käsittely perustuu muuhun oikeusperusteeseen, kuten yleistä etua koskevan tehtävän suorittamiseen (yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohta), Euroopan tietosuojaneuvosto suosittelee, että rekisteröidyt otetaan mukaan tutkimukseen vapaaehtoisuuden pohjalta.

3.3.2 Kerätyt tiedot

152. Rekisterinpitäjä saa kerätä ainoastaan henkilötietoja, jotka ovat käsittelyn kannalta ehdottoman välttämättömiä.

153. Huomioon otettavia tietoja on kahdenlaisia:

- **osallistujia ja ajoneuvoja koskevat tiedot**;
- **ajoneuvojen tekniset tiedot** (kuten hetkellinen nopeus).

154. Onnettomuuksiin liittyvä tieteellinen tutkimus oikeuttaa myös sellaiset oikeushenkilöt keräämään hetkellistä nopeutta koskevia tietoja, jotka eivät varsinaisesti hallinnoi julkista palvelua.

155. Kuten edellä on todettu, Euroopan tietosuojaneuvosto katsoo, että onnettomuustutkimuksen yhteydessä kerätyt tiedot ajoneuvon hetkellisestä nopeudesta eivät niiden käyttötarkoituksen perusteella ole rikkomukseen liittyviä tietoja (niitä ei kerätä rikostutkintaa ja syytetoimia varten), ja näin ollen oikeushenkilöt, jotka eivät varsinaisesti hallinnoi julkista palvelua, voivat kerätä kyseisiä tietoja.

3.3.3 Säilytysaika

156. On tärkeää erottaa toisistaan kaksi tietotyyppiä. Ensinnäkin osallistujia ja ajoneuvoja koskevia tietoja voidaan säilyttää koko tutkimuksen ajan. Toiseksi ajoneuvojen teknisiä tietoja olisi säilytettävä tähän tarkoitukseen mahdollisimman lyhyen ajan. Viisi vuotta tutkimuksen päättymispäivästä vaikuttaa tältä osin olevan kohtuullinen aika. Kyseisen ajanjakson jälkeen tiedot on poistettava tai anonymisoitava.

3.3.4 Tietojen antaminen ja rekisteröityjen oikeudet

157. Rekisteröidylle on ennen henkilötietojen käsittelyä ilmoitettava asiasta yleisen tietosuoja-asetuksen 13 artiklan mukaisesti läpinäkyvällä ja ymmärrettävällä tavalla. Erityisesti silloin, kun on kyse hetkellistä nopeutta koskevan tiedon keräämisestä, rekisteröidyille olisi ilmoitettava nimenomaisesti tietojen keräämisestä. Koska tietojenkäsittely perustuu suostumukseen, rekisteröidylle on ilmoitettava nimenomaisesti hänen oikeudestaan peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Koska tässä yhteydessä kerätyt tiedot antaa rekisteröity (tätä varten tarkoitetuissa lomakkeissa tai toimintansa myötä) ja niitä käsitellään yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohdan (suostumus) perusteella, rekisteröidyllä on oikeus käyttää oikeuttaan tietojen siirtämiseen järjestelmästä toiseen. Euroopan tietosuojaneuvosto suosittelee painokkaasti, kuten oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevissa ohjeissa korostetaan, että ”rekisterinpitäjät selittävät selvästi niiden tietojen välisen eron, jotka rekisteröity voi saada tietoon pääsyä ja tietojen siirtämistä koskevien oikeuksien perusteella”. Näin ollen rekisterinpitäjän olisi tarjottava helppo tapa peruuttaa suostumus vapaaehtoisesti ja milloin tahansa sekä kehitettävä välineitä, joiden avulla voidaan vastata tietojen siirtämistä järjestelmästä toiseen koskeviin pyyntöihin.

158. Nämä tiedot voidaan antaa allekirjoitettaessa lomaketta, jossa suostutaan osallistumaan onnettomuustutkimukseen.

3.3.5 Vastaanottaja

159. Periaatteessa ainoastaan rekisterinpitäjällä ja henkilötietojen käsittelijällä on pääsy tietoihin.

3.3.6 Turvallisuus

160. Kuten edellä todettiin, käyttöön otetut turvatoimet on mukautettava tietojen arkaluonteisuuden tason mukaan. Euroopan tietosuojaneuvosto suosittaa painokkaasti, että jos esimerkiksi onnettomuustutkimuksen yhteydessä kerätään hetkellistä nopeutta koskevia tietoja (tai muita rikostuomioihin ja rikkomuksiin liittyviä tietoja), käyttöön otetaan tehokkaita turvatoimia, joita ovat muun muassa

- pseudonymisointiin liittyvien toimenpiteiden toteuttaminen (esim. yksityisen avaimen hajauttaminen esimerkiksi rekisteröidyn sukunimen/etunimen ja sarjanumeron kaltaisten tietojen osalta);
- hetkelliseen nopeuteen ja sijaintiin liittyvien tietojen tallentaminen eri tietokantoihin (esim. käyttämällä huipputason salausmekanismia, johon liittyy erilliset avaimet ja hyväksyntämekanismit);
- ja/tai sijaintitietojen poistaminen heti, kun kyseessä oleva tapahtuma tai tapahtumasarja on vahvistettu (esim. tietyyppi, päivä/yö), ja suoraan tunnistettavien tietojen tallentaminen erilliseen tietokantaan, johon vain pienellä määrällä ihmisiä on pääsy.

3.4 Autovarkauksien torjuminen

161. Mikäli ajoneuvo varastetaan, rekisteröidyt saattavat haluta yrittää löytää ajoneuvonsa paikannuksen avulla. Sijaintitietojen käyttö on rajoitettu siihen, mikä on ehdottoman tarpeen tutkintaa ja toimivaltaisten oikeusviranomaisten suorittaman tapauksen arviointia varten.

3.4.1 Oikeusperuste

162. Kun tiedot kerätään yleisesti saatavilla olevan sähköisen viestintäpalvelun kautta, sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa.

163. Koska kyseessä on tietoyhteiskuntapalvelu, sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa ei edellytetä suostumusta ajoneuvoon tallennettujen tietojen käyttöön, kun tilaaja erityisesti pyytää tällaista palvelua.

164. Mitä tulee henkilötietojen käsittelyyn, sijaintitietojen käsittelyn oikeusperusteena on ajoneuvon omistajan suostumus tai sovellettavissa tapauksissa sopimuksen täytäntöönpano (ainoastaan sellaisten henkilötietojen osalta, jotka ovat tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena).

165. Suostumuksen on ilmennettävä sen henkilön vapaata, yksilöityä ja tietoista tahtoa, jonka tietoja käsitellään (esim. rastitetaan ruutu, jota ei ole valmiiksi rastitettu, tai määritetään kojelautatietokone toiminnon aktivoimiseksi ajoneuvossa). Suostumuksen vapaaehtoisuuteen sisältyy mahdollisuus peruuttaa suostumus milloin tahansa, ja rekisteröidylle olisi nimenomaisesti ilmoitettava asiasta. Suostumuksen peruuttamisen on johdettava käsittelyn lopettamiseen. Tämän jälkeen tiedot olisi poistettava aktiivisesta tietokannasta, anonymisoitava tai arkistoitava.

3.4.2 Kerätyt tiedot

166. Sijaintitietoja voidaan lähettää ainoastaan sen jälkeen, kun varkaudesta on ilmoitettu, eikä niitä voida kerätä keskeytyksettä muuna aikana.

3.4.3 Säilytysaika

167. Sijaintitietoja voidaan säilyttää ainoastaan sen ajanjakson ajan, jona toimivaltaiset oikeusviranomaiset arvioivat tapausta, tai sellaisen epäilyjen hälventämiseen liittyvän menettelyn päättymiseen saakka, joka ei vahvista ajoneuvon varkautta.

3.4.4 Rekisteröidylle ilmoittaminen

168. Rekisteröidylle olisi ennen henkilötietojen käsittelyä ilmoitettava asiasta yleisen tietosuoja-asetuksen 13 artiklan mukaisesti läpinäkyvällä ja ymmärrettävällä tavalla. Tietosuojaneuvosto suosittelee erityisesti, että rekisterinpitäjä korostaa, että ajoneuvoa ei seurata jatkuvasti ja että sijaintitiedot voidaan kerätä ja toimittaa vasta varkaudesta ilmoittamisen jälkeen. Rekisterinpitäjän on lisäksi annettava rekisteröidylle tiedot siitä, että ainoastaan etävalvontajärjestelmän hyväksytyillä toimijoilla ja laillisesti hyväksytyillä viranomaisilla on pääsy tietoihin.

169. Rekisteröityjen oikeuksien osalta Euroopan tietosuojaneuvosto toteaa, että koska tietojenkäsittely perustuu suostumukseen, rekisteröidylle olisi ilmoitettava nimenomaisesti hänen oikeudestaan peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Koska tässä yhteydessä kerätyt tiedot antaa rekisteröity (tätä varten tarkoitetuissa lomakkeissa tai toimintansa myötä) ja niitä käsitellään yleisen tietosuoja-

asetuksen 6 artiklan 1 kohdan a alakohdan (suostumus) tai 6 artiklan 1 kohdan b alakohdan (sopimuksen täytäntöönpano) perusteella, rekisteröidyllä on lisäksi oikeus käyttää oikeuttaan tietojen siirtämiseen järjestelmästä toiseen. Euroopan tietosuojaneuvosto suosittelee painokkaasti, kuten oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevissa ohjeissa korostetaan, että ”rekisterinpitäjät selittävät selvästi niiden tietojen välisen eron, jotka rekisteröity voi saada tietoon pääsyä ja tietojen siirtämistä koskevien oikeuksien perusteella”.

170. Näin ollen rekisterinpitäjän olisi tarjottava helppo tapa peruuttaa suostumus (ainoastaan, kun suostumusta käytetään oikeusperusteena) vapaaehtoisesti ja milloin tahansa sekä kehitettävä välineitä, joiden avulla voidaan vastata tietojen siirtämistä järjestelmästä toiseen koskeviin pyyntöihin.

171. Tiedot voidaan antaa, kun sopimus allekirjoitetaan.

3.4.5 Vastaanottajat

172. Jos varkaudesta ilmoitetaan, sijaintitiedot voidaan välittää i) etävalvontajärjestelmän hyväksytyille toimijoille ja ii) laillisesti hyväksytyille viranomaisille.

3.4.6 Turvallisuus

173. Yleisiä suosituksia sovelletaan. Ks. kohta 2.7.