Smjernice 1/2020 o obradi osobnih podataka u kontekstu povezanih vozila i aplikacija povezanih s mobilnošću

Verzija 2.0

Donesene 9. ožujka 2021.

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

Povijest verzija

Verzija 2.0	9. ožujka 2021.	Donošenje Smjernica nakon javnog savjetovanja
Verzija 1.0	28. siječnja 2020.	Donošenje Smjernica za javno savjetovanje

Sadržaj

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: „Opća uredba o zaštiti podataka"),

uzimajući u obzir Sporazum o EGP-u, posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 12. i 22. svojeg Poslovnika,

DONIO JE SLJEDEĆE SMJERNICE:

1. UVOD

1. Automobil je simbol gospodarstva 20. stoljeća i jedan od masovnih potrošačkih proizvoda koji je utjecao na cijelo društvo. Često ga se povezuje s pojmom slobode i smatra se da je više od pukog prijevoznog sredstva. Automobili su privatni prostor u kojem osobe imaju svojevrsnu samostalnost u donošenju odluka bez ikakvih vanjskih utjecaja. U današnje vrijeme, kad su povezana vozila sve prisutnija u svakodnevnom životu, takva vizija više ne odgovara stvarnosti. Usluga povezivosti u vozilu brzo se širi iz luksuznih modela i vrhunskih marki u najprodavanije modele srednje klase, a vozila postaju golema čvorišta podataka. Sve se više povezuju ne samo vozila već i vozači i putnici. Mnogi modeli koji su posljednjih godina stavljeni na tržište imaju senzore i ugrađenu povezanu opremu, kojima se, radi jedinstvene identifikacije pojedinca, mogu prikupljati i bilježiti, među ostalim, performanse motora, vozačke navike, posjećene lokacije i potencijalno čak i pokreti očiju vozača, njegov puls ili biometrijski podaci[2].

2. Takva obrada podataka odvija se u složenom sustavu koji nije ograničen na tradicionalne aktere iz automobilske industrije, već ga oblikuju i novi akteri iz digitalnog gospodarstva. Ti novi akteri mogu nuditi usluge informativnog i zabavnog sadržaja, kao što su glazba na internetu, stanje na cestama i informacije o prometu, ili pružati sustave i usluge pomoći u vožnji, kao što su softveri za automatski pilot, ažuriranje stanja vozila, osiguranje utemeljeno na upotrebi ili dinamičko mapiranje. Nadalje, budući da su vozila povezana elektroničkim komunikacijskim mrežama, upravitelji cestovne infrastrukture i telekomunikacijski operatori koji su uključeni u taj proces isto tako imaju važnu ulogu s obzirom na potencijalne postupke obrade koji se primjenjuju na osobne podatke vozača i putnika.

3. Povezana vozila generiraju sve veće količine podataka, od kojih se većina može smatrati osobnim podacima jer će se odnositi na vozače ili putnike. Čak i ako podaci prikupljeni povezanim automobilom nisu izravno povezani s imenom, već s tehničkim aspektima i značajkama vozila, oni će se odnositi na vozača ili putnike u automobilu. Primjerice, podaci koji se odnose na način vožnje, prijeđenu udaljenost, trošenje i habanje dijelova vozila, podaci o lokaciji ili podaci prikupljeni kamerama mogu se odnositi na ponašanje vozača i na informacije o drugim osobama u vozilu ili ispitanicima koji su tek prolaznici. Takve tehničke podatke, koji omogućuju izravno ili neizravno utvrđivanje identiteta pojedinca, proizvodi

[1] Upućivanja na „države članice" u ovom dokumentu trebaju se tumačiti kao upućivanja na „države članice EGP-a".
[2] Infografika „Podaci i povezani automobil" Foruma o budućnosti privatnosti; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

pojedinac, voditelj obrade podataka ili druga osoba. Vozilo se smatra terminalom koji mogu upotrebljavati razni korisnici. Stoga, kad je riječ o osobnom računalu, taj potencijalni veći broj korisnika ne utječe na to što se smatra osobnim podacima.

4. Međunarodna automobilistička federacija (FIA) 2016. je vodila kampanju u cijeloj Europi pod nazivom „Moj automobil, moji podaci" kako bi saznala što Europljani misle o povezanim automobilima[3]. Iako je pokazala velik interes vozača za povezivost, istaknula je i da treba biti posebno oprezan pri upotrebi podataka proizvedenih u vozilima te da je važno poštovati zakonodavstvo o zaštiti osobnih podataka. Stoga je izazov za svakog dionika uključiti dimenziju „zaštite osobnih podataka" u fazu dizajniranja proizvoda i osigurati korisnicima automobila transparentnost i kontrolu nad njihovim podacima u skladu s uvodnom izjavom 78. Opće uredbe o zaštiti podataka. Takvim pristupom pridonosi se jačanju povjerenja korisnika, a time i dugoročnom razvoju tih tehnologija.

1.1. Povezani radovi

5. U posljednjem desetljeću, a posebice posljednjih nekoliko godina, regulatori se sve više bave povezanim vozilima. Stoga su na nacionalnoj i međunarodnoj razini objavljeni razni radovi o sigurnosti i privatnosti povezanih vozila. Cilj je tih propisa i inicijativa nadopuniti postojeće okvire za zaštitu podataka i privatnost posebnim pravilima za pojedine sektore ili izraditi smjernice za profesionalce.

1.1.1. Inicijative na europskoj razini i međunarodne inicijative

6. Od 31. ožujka 2018. sustav eCall (e-poziv) ugrađen u vozilo koji se temelji na službi 112 obavezan je za sve nove kategorije vozila M1 i N1 (osobne automobile i laka gospodarska vozila)[4,5]. Radna skupina iz članka 29. već je 2006. objavila radni dokument o posljedicama na zaštitu podataka i privatnost u okviru inicijative eCall[6]. Osim toga, kako je prethodno navedeno, Radna skupina iz članka 29. donijela je u listopadu 2017. mišljenje o obradi osobnih podataka u kontekstu kooperativnih inteligentnih prometnih sustava (C-ITS).

7. U siječnju 2017. Agencija Europske unije za mrežnu i informacijsku sigurnosti (ENISA) objavila je studiju o kibersigurnosti i otpornosti pametnih automobila u kojoj je navela osjetljive resurse i povezane prijetnje, rizike, čimbenike ublažavanja rizika i sigurnosne mjere koje bi se mogle provesti[7]. Na Međunarodnoj konferenciji povjerenika za zaštitu podataka i privatnosti (ICDPPC) koja je održana u rujnu 2017. donesena je rezolucija o povezanim vozilima[8]. Naposljetku, u travnju 2018. i Međunarodna radna skupina za zaštitu podataka u telekomunikacijama (IWGDPT) objavila je radni dokument o povezanim vozilima.[9]

1.1.2. Nacionalne inicijative članova Europskog odbora za zaštitu podataka (Odbor)

8. U siječnju 2016. Konferencija njemačkih saveznih i državnih tijela za zaštitu podataka i Njemačko udruženje automobilske industrije (VDA) objavili su zajedničku deklaraciju o

[3] Kampanja „Moj automobil, moji podaci": http://www.mycarmydata.eu/.
[4] Interoperabilni sustav eCall na području cijele Europske unije: https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_hr
[5] Odluka br. 585/2014/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o uvođenju interoperabilne usluge e-poziva (eCall) na području cijele Europske unije (Tekst značajan za EGP): https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32014D0585
[6] Radni dokument o posljedicama na zaštitu podataka i privatnost u okviru inicijative eCall: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.
[7] Kibersigurnost i otpornost pametnih automobila: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[8] Rezolucija o zaštiti podataka u automatiziranim i povezanim vozilima: https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf
[9] Radni dokument o povezanim vozilima: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/

načelima zaštite podataka u povezanim i nepovezanim vozilima[10]. U kolovozu 2017. Centar Ujedinjene Kraljevine za povezana i automatizirana vozila (CCAV) objavio je vodič u kojem se navode načela kibersigurnosti za povezana i automatizirana vozila kako bi se skrenula pozornost na to pitanje u automobilskom sektoru[11]. U listopadu 2017. francusko tijelo za zaštitu podataka Commission Nationale de l'Informatique et des Libertés (CNIL) objavilo je paket mjera za područje sukladnosti za povezane automobile kako bi dionicima pružila pomoć u uvođenju tehničke i integrirane zaštite podataka i na taj način ispitanicima omogućila učinkovita kontrola nad njihovim podacima[12].

1.2. Mjerodavno pravo

9. Opća uredba o zaštiti podataka čini relevantni pravni okvir EU-a. Primjenjuje se u svakom slučaju kad obrada podataka u kontekstu povezanih vozila uključuje obradu osobnih podataka pojedinaca.

10. Uz Opću uredbu o zaštiti podataka Direktivom 2002/58/EZ, kako je izmijenjena Direktivom 2009/136/EZ (dalje u tekstu: „Direktiva o e-privatnosti"), **utvrđuje se poseban standard za sve aktere koji žele pohraniti podatke ili pristupiti podacima pohranjenima na terminalnoj opremi pretplatnika ili korisnika u Europskom gospodarskom prostoru (EGP).**

11. Ako se većina odredbi Direktive o e-privatnosti (članak 6., članak 9. itd.) primjenjuje samo na davatelje javno dostupnih elektroničkih komunikacijskih usluga i davatelje javnih komunikacijskih mreža, članak 5. stavak 3. Direktive o e-privatnosti čini opću odredbu. Ne primjenjuje se samo na elektroničke komunikacijske usluge već i na svaki privatni ili javni subjekt koji postavlja podatke na terminalnu opremu ili ih očitava s nje bez obzira na vrstu podataka koji se pohranjuju ili kojima se pristupa.

12. Pojam „terminalna oprema" definiran je u Direktivi 2008/63/EZ[13]. Terminalna oprema definirana je u članku 1. točki (a) kao „oprema koja je izravno ili neizravno povezana sa sučeljem javne telekomunikacijske mreže s ciljem slanja, obrade ili primanja informacija; u svakom slučaju (izravno ili neizravno), povezivanje se može ostvariti žicom, optičkim vlaknom ili elektromagnetski; povezivanje je neizravno ako je oprema smještena između terminala i sučelja mreže; (b) oprema za zemaljsku satelitsku stanicu".

13. Ako su ispunjeni prethodno navedeni kriteriji, povezano vozilo i na njega povezani uređaj stoga bi se trebali smatrati „terminalnom opremom" (baš kao i računalo, pametni telefon ili pametni televizor) te se odredbe članka 5. stavka 3. Direktive o e-privatnosti primjenjuju prema potrebi.

14. Kao što je Odbor istaknuo u svojem mišljenju 5/2019 o povezanosti Direktive o e-privatnosti i Opće uredbe o zaštiti podataka[14], u članku 5. stavku 3. Direktive o e-privatnosti propisuje se, uz iznimke navedene u točki 17. u nastavku, prethodni pristanak za pohranu informacija ili za pristup informacijama koje su već pohranjene na terminalnoj opremi pretplatnika ili

[10] Aspekti zaštite podataka pri upotrebi povezanih i nepovezanih vozila: https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf
[11] Načela kibersigurnosti za povezana i automatizirana vozila: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles
[12] Paket mjera za područje sukladnosti za odgovornu upotrebu podataka u povezanim automobilima: https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data
[13] Direktiva Komisije 2008/63/EZ od 20. lipnja 2008. o tržišnom natjecanju na tržištima telekomunikacijske terminalne opreme (Kodificirana inačica) (Tekst značajan za EGP): https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A32008L0063
[14] Europski odbor za zaštitu podataka, Mišljenje 5/2019 o povezanosti Direktive o e-privatnosti i Opće uredbe o zaštiti podataka, posebice u vezi s nadležnosti, zadaćama i ovlastima tijela za zaštitu podataka, doneseno 12. ožujka 2019. (dalje u tekstu: „Mišljenje 5/2019"), stavak 40.

korisnika. U mjeri u kojoj su informacije pohranjene u uređaju krajnjeg korisnika osobni podaci, članak 5. stavak 3. Direktive o e-privatnosti ima prednost pred člankom 6. Opće uredbe o zaštiti podataka kad je riječ o pohrani informacija ili pristupu tim informacijama[15]. Nakon prethodno navedenih postupaka obrade svi postupci obrade osobnih podataka, uključujući obradu osobnih podataka dobivenih pristupom informacijama na terminalnoj opremi, moraju imati pravnu osnovu u skladu s člankom 6. Opće uredbe o zaštiti podataka kako bi bili zakoniti[16].

15. Budući da će voditelj obrade pri traženju pristanka za pohranu ili pristup informacijama u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti morati obavijestiti ispitanika o svim svrhama obrade, uključujući bilo kakvu obradu nakon prethodno navedenih postupaka („naknadna obrada"), privola u skladu s člankom 6. Opće uredbe o zaštiti podataka bit će općenito najprikladnija pravna osnova za obradu osobnih podataka nakon takvih postupaka (ako je svrha daljnje obrade obuhvaćena privolom ispitanika, vidjeti točke 53. – 54. u nastavku). Stoga će pristanak vjerojatno biti pravna osnova za pohranu informacija i pristup već pohranjenim informacijama i naknadnu obradu osobnih podataka[17]. Pri procjeni usklađenosti s člankom 6. Opće uredbe o zaštiti podataka trebalo bi uzeti u obzir da cjelokupna obrada uključuje određene aktivnosti za koje zakonodavac EU-a nastoji pružiti dodatnu zaštitu[18]. Nadalje, kako bi se poštovalo načelo pravednosti, voditelji obrade trebali bi pri utvrđivanju odgovarajuće pravne osnove uzeti u obzir učinak na prava ispitanika.[19] Bit je u tome da se voditelji obrade ne mogu pozvati na članak 6. Opće uredbe o zaštiti podataka kako bi smanjili dodatnu zaštitu predviđenu člankom 5. stavkom 3. Direktive o e-privatnosti.

16. Odbor podsjeća da je pojam pristanka u Direktivi o e-privatnosti i dalje isti kao pojam privole u Općoj uredbi o zaštiti podataka te mora ispunjavati sve zahtjeve privole predviđene člankom 4. točkom 11. i člankom 7. Opće uredbe o zaštiti podataka.

17. Međutim, iako se načelno primjenjuje pristanak, člankom 5. stavkom 3. Direktive o e-privatnosti dopušta se da se pohrana informacija ili pristup informacijama koje su već pohranjene na terminalnoj opremi izuzme od zahtjeva za informirani pristanak ako je ispunjen jedan od sljedećih kriterija:

- **iznimka 1:** isključivo u svrhu prijenosa komunikacije putem elektroničke komunikacijske mreže
- **iznimka 2:** ako je neophodno za pružanje određene usluge informacijskog društva koju je pretplatnik ili korisnik izričito zatražio od davatelja te usluge.

18. U takvim se slučajevima obrada osobnih podataka, uključujući osobne podatke dobivene pristupom informacijama na terminalnoj opremi, temelji na jednoj od pravnih osnova predviđenih člankom 6. Opće uredbe o zaštiti podataka. Primjerice, pristanak nije potreban ako je obrada podataka nužna da bi se ispitaniku koji ih je zatražio mogle pružiti GPS navigacijske usluge koje se mogu opisati kao usluge informacijskog društva.

1.3. Područje primjene

19. Odbor ističe da se ovim smjernicama želi olakšati usklađenost obrade osobnih podataka koju provode brojni dionici koji rade u predmetnom okruženju. Međutim, njima se ne

[15] Vidjeti bilješku 14., stranica 7., stavak 40.
[16] Vidjeti bilješku 14., stranica 7., stavak 41.
[17] Pristanak u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti i privola koja je pravna osnova za obradu podataka (članak 6. Opće uredbe o zaštiti podataka) mogu se prikupljati u istu svrhu i u isto vrijeme (primjerice, označivanjem kućice kojim se jasno ukazuje na što ispitanik pristaje).
[18] Mišljenje 5/2019, stavak 41.
[19] Europski odbor za zaštitu podataka, Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke (b) Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, verzija 2.0, 8. listopada 2019., točka 1.

namjeravaju obuhvatiti svi mogući slučajevi u danom kontekstu ili dati upute za svaku moguću posebnu situaciju.

20. Područje primjene ovog dokumenta posebno je usmjereno na obradu osobnih podataka koja se odnosi na neprofesionalne korisnike povezanih vozila: npr. vozače, putnike, vlasnike vozila, druge sudionike u cestovnom prometu itd. Točnije, obuhvaća osobne podatke: i. koji su obrađeni u vozilu, ii. koji su razmijenjeni između vozila i osobnih uređaja povezanih s njime (npr. korisnikov pametni telefon) ili iii. koji su prikupljeni lokalno u vozilu i izvezeni vanjskim subjektima (npr. proizvođači vozila, upravitelji infrastrukture, društva za osiguranje, automehaničari) radi daljnje obrade.

21. Povezano vozilo u ovom dokumentu ima široko značenje. Može se definirati kao vozilo opremljeno mnogim elektroničkim upravljačkim jedinicama (ECU), koje su međusobno povezane putem mreže vozila, i uređajima za povezivanje koji omogućavaju razmjenu informacija s drugim uređajima unutar i izvan vozila. Podaci se kao takvi mogu razmjenjivati između vozila i drugih s njime povezanih osobnih uređaja, primjerice tako da se omogući zrcaljenje mobilnih aplikacija na jedinicu za informativni i zabavni sadržaj na upravljačkoj ploči automobila. Nadalje, razvoj samostalnih mobilnih aplikacija za pomoć vozačima, dakle aplikacija neovisnih o vozilu (primjerice, koje se oslanjaju isključivo na upotrebu pametnog telefona) obuhvaćen je područjem primjene ovog dokumenta jer pridonosi mogućnostima povezivosti vozila iako se te aplikacije same po sebi u stvarnosti ne oslanjaju na prijenos podataka vozilom. Postoje brojne raznolike aplikacije za povezana vozila, a mogu uključivati[20]:

22. *Upravljanje mobilnošću:* funkcije koje omogućavaju vozačima da na brz i troškovno učinkovit način dođu do odredišta te im pravodobno pružaju informacije o GPS navigaciji, potencijalno opasnim uvjetima iz okoline (npr. zaleđene ceste), zagušenjima u prometu ili građevinskim radovima na izgradnji cesta, dostupnim parkirališima ili garažama, optimiziranoj potrošnji goriva ili cijenama cestarina.

23. *Upravljanje vozilom:* funkcije koje bi trebale pomoći vozačima u smanjenju operativnih troškova i poboljšanju jednostavnosti upotrebe, kao što su obavijesti o stanju vozila i podsjetnici na servis, prijenos podataka o upotrebi (npr. za usluge popravka vozila), prilagođena osiguranja „plati koliko/kako voziš", daljinsko upravljanje (npr. sustav grijanja) ili konfiguracije profila (npr. položaj sjedala).

24. *Sigurnost na cestama:* funkcije koje upozoravaju vozača na vanjske opasnosti i reakcije sustava vozila, kao što su zaštita od sudara, upozorenja na opasnost, upozorenja o napuštanju prometne trake, prepoznavanje umornog vozača, hitni poziv (eCall) ili „crne kutije" za istraživanje nesreće (uređaji za snimanje podataka o događaju).

25. *Zabavni sadržaj:* funkcije koje pružaju informacije i uključuju usluge zabavnog sadržaja za vozača i putnike, kao što su sučelja pametnih telefona (obavljanje telefonskih poziva bez ruku, glasovno pisanje poruka), WLAN pristupne točke, glazba, videozapisi, internet, društveni mediji, mobilni uredi ili usluge za „pametni dom".

26. *Pomoć vozaču:* funkcije koje uključuju djelomično ili potpuno automatiziranu vožnju, kao što je operativna pomoć ili automatski pilot u gustom prometu, na parkiralištu ili na autocestama.

27. *Dobrobit:* funkcije koje nadziru udobnost vozača i njegovu sposobnost za upravljanje vozilom, kao što su prepoznavanje umora ili liječnička pomoć.

[20] Strategija PwC-a iz 2014. *In the fast lane. The bright future of connected cars* (U brzoj traci. Svijetla budućnost povezanih automobila): https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

28. Stoga se vozila mogu ili ne moraju automatski povezati, a osobni podaci mogu se prikupljati na nekoliko načina, među ostalim: i. senzorima vozila, ii. telematičkim kutijama ili iii. mobilnim aplikacijama (npr. kojima se pristupa s uređaja koji pripada vozaču). Aplikacije moraju biti povezane s voznom okolinom kako bi bile obuhvaćene područjem primjene ovog dokumenta. Primjerice, aplikacije za GPS navigaciju obuhvaćene su područjem primjene. Međutim, aplikacije s funkcijama koje vozačima samo predlažu zanimljiva mjesta (restorani, povijesni spomenici itd.) nisu obuhvaćene područjem primjene ovih smjernica.

29. Većina podataka koji su proizvedeni povezanim vozilom odnosi se na pojedinca čiji je identitet utvrđen ili se može utvrditi i stoga se smatraju osobnim podacima. Primjerice, podaci uključuju podatke iz kojih se može izravno utvrditi identitet (npr. cjelokupni identitet vozača) i podatke iz kojih se može neizravno utvrditi identitet, kao što su pojedinosti o obavljenim putovanjima, podaci o upotrebi vozila (npr. podaci o načinu vožnje ili prijeđenoj udaljenosti) ili tehnički podaci o vozilu (npr. podaci o trošenju i habanju dijelova vozila), i koji se unakrsnim upućivanjem na druge datoteke i posebice na identifikacijski broj vozila (VIN) mogu povezati s pojedincem. Osobni podaci u povezanim vozilima mogu uključivati i metapodatke, kao što je status održavanja vozila. Drugim riječima, svi podaci koji se mogu povezati s pojedincem stoga su obuhvaćeni područjem primjene ovog dokumenta.

30. Ekosustav povezanih vozila obuhvaća široki spektar dionika. Konkretno, taj ekosustav uključuje tradicionalne aktere automobilske industrije i nove aktere iz digitalne industrije. Stoga su ove smjernice namijenjene proizvođačima vozila, proizvođačima opreme i dobavljačima za automobilsku industriju, automehaničarima, prodavaonicama automobila, davateljima usluga servisiranja vozila, upraviteljima voznih parkova, društvima za osiguranje motornih vozila, davateljima usluga zabavnog sadržaja, telekomunikacijskim operaterima, upraviteljima cestovne infrastrukture i javnim tijelima, ali i ispitanicima. Odbor naglašava da će se kategorije ispitanika razlikovati ovisno o usluzi (npr. vozači, vlasnici, putnici itd.). Ovaj potpis nije potpun jer ekosustav uključuje brojne usluge, uključujući usluge za koje je potrebna izravna autentifikacija ili identifikacija te usluge za koje to nije potrebno.

31. Stoga neke obrade osobnih podataka u vozilu koje pojedinci obavljaju „u okviru isključivo osobne ili kućne aktivnosti" nisu obuhvaćene područjem primjene Opće uredbe o zaštiti podataka[21]. To se posebno odnosi na upotrebu osobnih podataka unutar vozila, a tim se podacima koriste isključivo ispitanici koji su postavili te podatke u upravljačku ploču vozila. Međutim, Odbor podsjeća da se, u skladu s uvodnom izjavom 18. Opće uredbe za zaštitu podataka, ona „primjenjuje na voditelje obrade ili izvršitelje obrade koji pružaju sredstva za obradu osobnih podataka za takve osobne ili kućne aktivnosti".

1.3.1. Izvan područja primjene ovog dokumenta

32. Moguće je da će poslodavci koji osiguravaju službene automobile za zaposlenike htjeti nadzirati njihove aktivnosti (primjerice, kako bi se osigurala sigurnost zaposlenika, robe ili vozila, dodijelila sredstva, pratila i naplatila usluga ili provjerilo radno vrijeme). Obrada podataka koju u tom kontekstu provode poslodavci otvara posebna pitanja u kontekstu zapošljavanja, koja bi mogla biti uređena nacionalnim zakonodavstvom o radu koje se ne može detaljno opisati u ovim smjernicama[22].

33. Iako se zbog obrade podataka u gospodarskim vozilima koja se upotrebljavaju u profesionalne svrhe (kao što je javni prijevoz) i u okviru zajedničkog prijevoza i rješenja platforme MaaS mogu otvoriti važna pitanja koja nisu obuhvaćena područjem primjene ovih općih smjernica, mnoga načela i preporuke koje su ovdje utvrđene mogu se primijeniti i na te vrste obrade.

[21] Vidjeti članak 2. stavak 2. točku (c) Opće uredbe o zaštiti podataka.
[22] Radna skupina iz članka 29. to je razradila u svojem Mišljenju 2/2017 o obradi podataka na radnome mjestu, WP249: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

34. Budući da su povezana vozila sustavi s radijem, podliježu pasivnom praćenju, kao što su praćenje putem Wi-Fi mreže ili Bluetooth signala. U tom se smislu ne razlikuju od ostalih povezanih uređaja i obuhvaćeni su područjem primjene Direktive o e-privatnosti koja se trenutačno revidira. Stoga se time isključuje opsežno praćenje vozila opremljenih Wi-Fi mrežom[23] koje provodi gusta mreža prolaznika koji upotrebljavaju uobičajene usluge lokacije pametnih telefona. Njima se sve vidljive Wi-Fi mreže rutinski prijavljuju središnjim poslužiteljima. Budući da se ugrađena Wi-Fi mreža može smatrati sekundarnim identifikatorom vozila[24], postoje rizici od sustavnog i stalnog prikupljanja cjelovitog profila kretanja vozila.

35. Vozila se sve češće opremaju uređajima za snimanje slike (npr. sustavi kamera za parkiranje ili kamere u vozilima). Budući da se to odnosi na snimanje javnih mjesta, pa bi trebalo procijeniti relevantne zakonodavne okvire svojstvene za svaku državu članicu, ta obrada podataka nije obuhvaćena područjem primjene ovih smjernica.

36. Obrada podataka koja omogućuje funkcioniranje kooperativnih inteligentnih prometnih sustava (C-ITS), kako su utvrđeni u Direktivi 2010/40/EU[25], razrađena je u posebnom mišljenju Radne skupine iz članka 29.[26] Iako se u definiciji koncepta C-ITS-a u direktivi ne navode tehničke specifikacije, Radna skupina iz članka 29. u svojem se mišljenju usredotočila na komunikaciju kratkog dometa, tj. onu koja ne uključuje intervenciju mrežnog operatera. Konkretnije, analizirala je posebne slučajeve upotrebe za početno uvođenje i obvezala se da će kasnije procijeniti nova pitanja koja će se nedvojbeno pojaviti nakon što se postigne viša razina automatizacije. Budući da su učinci na zaštitu podataka u kontekstu C-ITS-a vrlo svojstveni (dosad najveća količina podataka o lokaciji, stalno emitiranje osobnih podataka, razmjena podataka između vozila i drugih objekata cestovne infrastrukture itd.) i da se o tome i dalje raspravlja na europskoj razini, obrada osobnih podataka u tom kontekstu nije obuhvaćena ovim smjernicama.

37. Naposljetku, ovim dokumentom ne nastoje se riješiti svi mogući problemi i pitanja koja se odnose na povezana vozila i stoga ga se ne može smatrati potpunim.

1.4. Definicije

38. **Obrada** osobnih podataka obuhvaća svaki postupak koji uključuje osobne podatke, kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prijenosom, širenjem ili stavljanje na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje itd.[27]

39. **Ispitanik** je pojedinac na kojeg se odnose podaci obuhvaćeni obradom. U kontekstu povezanih vozila to posebice može biti vozač (stalni ili povremeni), putnik ili vlasnik vozila[28].

---

[23] Za pojedinosti vidjeti: 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 i Gerd Nolden, *Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings* (Identifikacija vozila na temelju sekundarnog identifikatora vozila – analiza i mjerenja), Zbornik radova VEHICULAR 2017: Šesta međunarodna konferencija o napretku u sustavima vozila, tehnologijama i aplikacijama, Nica, Francuska, 23. – 27. srpnja 2017., str. 32–37.

[25] Direktiva 2010/40/EU od 7. srpnja 2010. o okviru za uvođenje inteligentnih prometnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32010L0040

[26] Radna skupina iz članka 29. – Mišljenje 03/2017 o obradi osobnih podataka u kontekstu kooperativnih inteligentnih prometnih sustava (C-ITS): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

[27] Vidjeti članak 4. točku 2. Opće uredbe o zaštiti podataka.

[28] Vidjeti članak 4. točku 1. Opće uredbe o zaštiti podataka.

40. **Voditelj obrade podataka** znači osoba koja određuje svrhe i sredstva obrade koja se obavlja u povezanim vozilima[29]. Voditelji obrade podataka mogu uključivati davatelje usluga koji obrađuju podatke o vozilu kako bi vozaču poslali prometne informacije, poruke o ekološkoj vožnji ili upozorenja povezana s funkcioniranjem vozila, društva za osiguranje koja nude ugovore o osiguranju „plati koliko voziš" ili proizvođače vozila koji radi poboljšanja njegove kvalitete prikupljaju podatke o trošenju i habanju dijelova vozila. U skladu s člankom 26. Opće uredbe o zaštiti podataka dva ili više voditelja obrade mogu zajednički odrediti svrhe i načine obrade i stoga se smatraju zajedničkim voditeljima obrade. U tom slučaju moraju jasno utvrditi svoje obaveze, osobito s obzirom na ostvarivanje prava ispitanika i dostavu informacija u skladu s člankom 13. i člankom 14. Opće uredbe o zaštiti podataka.

41. **Izvršitelj obrade podataka** znači svaka osoba koja obrađuje osobne podatke u ime voditelja obrade podataka.[30] Izvršitelj obrade podataka prikuplja i obrađuje podatke prema uputama voditelja obrade podataka, a da pritom ne upotrebljava te podatke za vlastite svrhe. Primjerice, u brojnim slučajevima proizvođači opreme i dobavljači za automobilsku industriju mogu obrađivatipodatke u ime proizvođača vozila (što ne znači da ne mogu biti voditelji obrade podataka u druge svrhe). Člankom 28. Opće uredbe o zaštiti podataka utvrđuju se obveze izvršitelja obrade podataka i od njih se zahtijeva provedba odgovarajućih tehničkih i organizacijskih mjera kako bi se zajamčila odgovarajuća razina sigurnosti s obzirom na rizik.

42. **Primatelj** znači fizička ili pravna osoba, javno tijelo, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana[31]. Primjerice, komercijalni partner davatelja usluga koji od davatelja usluga prima osobne podatke proizvedene u vozilu primatelj je osobnih podataka. Bez obzira na to djeluju li kao novi voditelj obrade podataka ili izvršitelj obrade podataka, moraju ispunjavati obaveze utvrđene Općom uredbom o zaštiti podataka.

43. Međutim, javna tijela koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima[32]. Obrada tih podataka koju obavljaju ta javna tijela mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade. Primjerice, tijela za izvršavanje zakonodavstva ovlaštene su treće strane kad zahtijevaju osobne podatke kao dio istrage u skladu s pravom Europske unije ili države članice.

[29] Vidjeti članak 4. točku 7. Opće uredbe o zaštiti podataka i Europski odbor za zaštitu podataka, Smjernice 7/2020 o pojmovima „voditelj obrade" i „izvršitelj obrade" iz Opće uredbe o zaštiti podataka (dalje u tekstu: „Smjernice 7/2020").
[30] Vidjeti članak 4. točku 8. Opće uredbe o zaštiti podataka i Smjernice 7/2020.
[31] Vidjeti članak 4. točku 9. Opće uredbe o zaštiti podataka i Smjernice 7/2020.
[32] Članak 4. točka 9. i uvodna izjava 31. Opće uredbe o zaštiti podataka.

1.5. Rizici za privatnost i zaštitu podataka

44. Radna skupina iz članka 29. već je u više navrata izrazila zabrinutost u pogledu sustavâ interneta stvari, koja se može primijeniti i na povezana vozila.[33] Pitanja koja su već istaknuta u pogledu interneta stvari, a odnose se na sigurnost i kontrolu podataka, još su osjetljivija u kontekstu povezanih vozila jer uključuju probleme povezane sa sigurnošću na cestama u okruženju koje se tradicionalno smatra izoliranim i zaštićenim od vanjskih utjecaja i u tom okruženju mogu utjecati na tjelesni integritet vozača.

45. Nadalje, povezana vozila otvaraju važna pitanja o zaštiti podataka i privatnosti u pogledu obrade podataka o lokaciji jer njezina sve veća intruzivnost može ugroziti trenutačne mogućnosti anonimnosti. Odbor želi naglasiti i skrenuti pozornost dionika na činjenicu da upotreba tehnologija koje se temelje na lokalizaciji zahtijeva provedbu posebnih zaštitnih mjera kako bi se spriječio nadzor pojedinaca i zloupotreba podataka.

1.5.1. Nedostatak kontrole i asimetričnost informacija

46. Vozači i putnici možda neće uvijek na odgovarajući način biti obaviješteni o obradi podataka koja se provodi u povezanom vozilu ili putem njega. Moguće je da će informacije dobiti samo vlasnik vozila, koji možda nije vozač, ili da se one neće dobiti na vrijeme. Dakle, postoji rizik da nema dovoljno funkcija ili opcija koje se nude za provedbu kontrole potrebne da bi osobe na koje se odnosi obrada iskoristile svoja prava na zaštitu podataka i privatnost. To je važno jer vozila tijekom svojeg vijeka trajanja mogu imati više od jednog vlasnika jer se prodaju ili daju u zakup, a ne zato što se kupuju.

47. Osim toga, komunikacija u vozilu može se pokrenuti automatski, ali i po zadanim postavkama, a da pojedinac toga nije svjestan. Korisniku će svakako biti izuzetno teško kontrolirati protok podataka jer nema mogućnost da učinkovito kontrolira kako vozilo i njegova povezana oprema komuniciraju. Bit će još teže kontrolirati njihovu naknadnu upotrebu, a time i spriječiti potencijalno povećanje broja funkcija.

1.5.2. Kvaliteta pristanka/privole korisnika

48. Kao što je protumačeno u smjernicama Odbora o privoli, Odbor naglašava da bi, kad se obrada podataka temelji na privoli, svi elementi valjane privole trebali biti ispunjeni, a to znači da je privola dobrovoljna, posebna i informirana te da nedvosmisleno izražava želje ispitanika[34]. Voditelji obrade podataka moraju obratiti osobitu pozornost na načine dobivanja valjanih privola različitih sudionika, kao što su vlasnici ili korisnici automobila. Takva se privola daje odvojeno, za posebne svrhe i ne može se dodati ugovoru o kupnji ili zakupu novog automobila. Ispitanici moraju moći povući privolu jednostavno kao što su je i dali.

49. Isto vrijedi i kad se pristanak mora dobiti u skladu sa zahtjevima iz Direktive o e-privatnosti, primjerice ako se informacije pohranjuju ili se pristupa informacijama već pohranjenima u vozilu kako je u određenim slučajevima propisano člankom 5. stavkom 3. Direktive o e-privatnosti. Kako je prethodno navedeno, pristanak se u tom kontekstu mora tumačiti s obzirom na Opću uredbu o zaštiti podataka.

50. U mnogim slučajevima korisnik možda nije svjestan obrade podataka koja se provodi u njegovu vozilu. Takav nedostatak informacija znatna je zapreka dokazivanju postojanja valjane privole u skladu s Općom uredbom o zaštiti podataka s obzirom na to da ona mora biti informirana. U takvim okolnostima privola se ne može smatrati pravnom osnovom za odgovarajuću obradu podataka u skladu s Općom uredbom o zaštiti podataka.

---

[33] Radna skupina iz članka 29., Mišljenje 8/2014 o nedavnom razvoju u području interneta stvari: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_hr.pdf

[34] Europski odbor za zaštitu podataka, Smjernice 5/2020 o privoli na temelju Uredbe 2016/679, verzija 1.1., 4. svibnja 2020. (dalje u tekstu: „Smjernice 5/2020").

51. Klasični mehanizmi za dobivanje pristanka/privole osobe mogu biti teško primjenjivi u području povezanih vozila, zbog čega se dobiva pristanak/privola „slabe kvalitete" koja se temelje na nedostatku informacija ili na nemogućnosti davanja preciznog pristanka/privole u skladu s preferencijama koje je osoba izrazila. Osim toga, u praksi bi moglo biti teško dobiti pristanak/privolu vozača i putnika koji nisu povezani s vlasnikom vozila u slučaju rabljenih, zakupljenih, iznajmljenih ili posuđenih vozila.

52. Čak i ako se u okviru Direktive o e-privatnosti ne zahtijeva pristanak ispitanika, voditelji obrade moraju odabrati pravnu osnovu iz članka 6. Opće uredbe o zaštiti podataka koja je u tom slučaju najprikladnija za obradu osobnih podataka.

1.5.3. Daljnja obrada osobnih podataka

53. Kad se podaci prikupljaju na temelju pristanka u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti ili jednog od izuzeća iz članka 5. stavka 3. te se naknadno obrađuju u skladu s člankom 6. Opće uredbe o zaštiti podataka, njihova daljnja obrada moguća je samo ako voditelj obrade traži dodatnu privolu za tu drugu svrhu ili ako može dokazati da se obrada temelji na pravu Unije ili države članice radi zaštite ciljeva iz članka 23. stavka 1. Opće uredbe o zaštiti podataka[35]. Odbor smatra da se u takvim slučajevima daljnja obrada ne može temeljiti na ispitivanju usklađenosti iz članka 6. stavka 4. Opće uredbe o zaštiti podataka jer bi to dovelo u pitanje standard zaštite podataka iz Direktive o e-privatnosti. Pristanak, kad je propisan Direktivom o e-privatnosti, mora biti poseban i informiran, što znači da ispitanici moraju biti upoznati sa svim svrhama obrade podataka i imati pravo odbiti određene svrhe[36]. Tumačenjem da se daljnja obrada može temeljiti na ispitivanju usklađenosti iz članka 6. stavka 4. Opće uredbe o zaštiti podataka izbjeglo bi se samo načelo zahtjevâ za privolu utvrđeno važećom direktivom.

54. Odbor podsjeća da se prvotnom privolom nikad neće opravdati nastavak obrade jer privola mora biti informirana i posebna kako bi bila valjana.

55. Primjerice, telemetrijski podaci koji se prikupljaju tijekom upotrebe vozila u svrhu održavanja ne smiju se bez pristanka/privole korisnika otkriti društvima za osiguranje motornih vozila u svrhu izrade profila vozača kako bi ta društva mogla nuditi police osiguranja koje se temelje na ponašanju u vožnji.

56. Nadalje, ako i kad su ispunjeni posebni uvjeti iz direktive o izvršavanju zakonodavstva, tijela za izvršavanje zakonodavstva mogu obrađivati podatke prikupljene povezanim vozilima kako bi otkrila prebrzu vožnju ili druge prekršaje. U tom će se slučaju smatrati da se ti podaci odnose na kaznene osude i kaznena djela u skladu s uvjetima utvrđenima u članku 10. Opće uredbe o zaštiti podataka i bilo kojem primjenjivom nacionalnom zakonodavstvu. Ako su ispunjeni posebni uvjeti za takvu obradu, proizvođači mogu dostaviti takve podatke tijelima za izvršavanje zakonodavstva. Odbor naglašava da obrada osobnih podataka isključivo u svrhu ispunjavanja zahtjeva koje podnose tijela za izvršavanje zakonodavstva ne predstavlja posebnu, izričitu i zakonitu svrhu u smislu članka 5. stavka 1. točke (b) Uredbe o zaštiti podataka. Kad su tijela za izvršavanje zakonodavstva za to ovlaštena zakonom, ona bi mogla biti treća strana u smislu članka 4. točke 10. Opće uredbe o zaštiti podataka i u tom bi slučaju proizvođači imali pravo dostaviti im sve podatke kojima raspolažu pod uvjetom da je to u skladu s odgovarajućim pravnim okvirom u svakoj državi članici.

1.5.4. Pretjerano prikupljanje podataka

57. S obzirom na to da se sve veći broj senzora postavlja u povezana vozila, postoji visok rizik od pretjeranog prikupljanja podataka u usporedbi s onim što je potrebno za ostvarenje svrhe.

[35] Vidjeti i Europski odbor za zaštitu podataka, Smjernice 10/2020 o ograničenjima iz članka 23. Opće uredbe o zaštiti podataka.
[36] Smjernice 5/2020, odjeljci 3.2. i 3.3.

58. Razvoj novih funkcija, točnije onih koje se temelje na algoritmima strojnog učenja, može iziskivati prikupljanje velike količine podataka tijekom dugog razdoblja.

1.5.5. Sigurnost osobnih podataka

59. Mnoštvo funkcija, usluga i sučelja (npr. internet, USB, RFID, Wi-Fi) koje nude povezana vozila povećava površinu napada i broj mogućih slabosti putem kojih bi osobni podaci mogli biti ugroženi. Za razliku od većine uređaja interneta stvari povezana vozila kritični su sustavi u kojima povreda sigurnosti može ugroziti život svojih korisnika i ljudi oko njih. Stoga je još važnije poduzeti mjere za sprečavanje rizika od hakera koji pokušavaju iskoristiti slabosti povezanih vozila.

60. Osim toga, osobni podaci koji su pohranjeni u vozilima ili/i na vanjskim lokacijama (npr. infrastrukture računalstva u oblaku) moraju biti primjereno zaštićeni od neovlaštenog pristupa. Primjerice, vozilo se tijekom održavanja treba predati tehničaru koji će morati pristupiti nekim tehničkim podacima vozila. Iako tehničar mora imati pristup tehničkim podacima, postoji mogućnost da bi mogao pokušati pristupiti svim podacima koji su pohranjeni u vozilu.

2. OPĆE PREPORUKE

61. Kako bi se ublažili rizici za prethodno utvrđene ispitanike, proizvođači vozila i opreme, davatelji usluga i svi drugi dionici koji mogu djelovati kao voditelji ili izvršitelji obrade podataka u pogledu povezanih vozila trebali bi slijediti sljedeće opće preporuke.

2.1. Kategorije podataka

62. Kao što je navedeno u uvodu, većina podataka iz povezanih vozila smatrat će se osobnim podacima u mjeri u kojoj ih je moguće povezati s jednim ili više pojedinaca čiji se identitet može utvrditi. To uključuje tehničke podatke o kretanju vozila (npr. brzina, prijeđena udaljenost) i stanju vozila (npr. temperatura rashladne tekućine motora, broj okretaja motora u minuti, tlak u gumama). Određenim podacima koje proizvode povezana vozila potrebno je posvetiti posebnu pozornost s obzirom na njihovu osjetljivost i/ili potencijalni učinak na prava i interese ispitanika. Dosad je Odbor utvrdio tri kategorije osobnih podataka kojima proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebaju posvetiti posebnu pozornost: podaci o lokaciji, biometrijski podaci (i bilo koja posebna kategorija podataka utvrđena člankom 9. Opće uredbe o zaštiti podataka) i podaci iz kojih bi se mogla otkriti kaznena djela ili prometni prekršaji.

2.1.1. Podaci o lokaciji

63. Pri prikupljanju osobnih podataka proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebaju imati na umu da podaci o lokaciji puno govore o životnim navikama ispitanika. Iz obavljenih se putovanja može zaključiti koje je mjesto rada i prebivališta vozača, kao i njemu zanimljiva mjesta (u slobodno vrijeme), a mogu se otkriti i potencijalno osjetljive informacije, na primjer vjeroispovijest na temelju mjesta bogoslužja ili spolna orijentacija na temelju posjećenih mjesta. U skladu s time proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebali bi biti posebno oprezni i ne bi smjeli prikupljati podatke o lokaciji, osim ako je to nužno u svrhu obrade. Primjerice, kad se postupak obrade sastoji od otkrivanja podataka o kretanju vozila, za izvršavanje obrade dovoljan je žiroskop i nema potrebe za prikupljanjem podataka o lokaciji.

64. Općenito, prikupljanje podataka o lokaciji mora isto tako biti u skladu sa sljedećim načelima:

- odgovarajuća konfiguracija učestalosti pristupa podacima o lokaciji koji se prikupljaju s obzirom na svrhu obrade te odgovarajuća konfiguracija razine njihove detaljnosti; primjerice, aplikacije za vrijeme i vremensku prognozu ne bi trebale imati pristup lokaciji vozila u svakom trenutku, čak i uz pristanak/privolu ispitanika

- dostava točnih informacija u svrhu obrade (npr. pohranjuje li se povijest lokacija, a ako se pohranjuje, koja je svrha pohrane)
- kad se obrada temelji na privoli, dobivanje valjane (dobrovoljna, posebna i informirana) privole koja se razlikuje od općih uvjeta prodaje ili upotrebe, primjerice na sučelju računala u vozilu
- aktiviranje lokacije samo kad korisnik pokrene funkciju koja zahtijeva prepoznavanje lokacije, a ne automatski i kontinuirano kad se automobil pokrene
- obavještavanje korisnika da je lokacija aktivirana, posebno upotrebom ikona (npr. strelica koja se pomiče preko zaslona)
- mogućnost deaktiviranja lokacije u bilo kojem trenutku
- utvrđivanje ograničenog razdoblja pohrane.

2.1.2. Biometrijski podaci

65. U kontekstu povezanih vozila biometrijski podaci koji se upotrebljavaju za jedinstvenu identifikaciju pojedinca mogu se obrađivati, u okviru članka 9. Opće uredbe o zaštiti podataka i nacionalnih izuzeća, među ostalim, kako bi se omogućio pristup vozilu, autentificirao vozač/vlasnik i/ili omogućio pristup postavkama i preferencijama vozačeva profila. Kad se razmatra upotreba biometrijskih podataka, jamčenje potpune kontrole ispitanika nad vlastitim podacima uključuje, s jedne strane, omogućavanje nebiometrijske alternative (npr. upotreba fizičkog ključa ili koda) bez dodatnih ograničenja (tj. upotreba biometrije ne bi trebala biti obavezna) i, s druge strane, pohranu i usporedbu biometrijskog modela u šifriranom obliku isključivo na lokalnoj razini, pri čemu vanjski terminal za očitanje/usporedbu ne obrađuje biometrijske podatke.

66. Kad je riječ o biometrijskim podacima[37], važno je osigurati dovoljnu pouzdanost rješenja za biometrijsku autentifikaciju, posebno poštovanjem sljedećih načela:

- Prilagodba primijenjenog biometrijskog rješenja (npr. postotak lažno pozitivnih i lažno negativnih rezultata) usklađuje se sa sigurnosnom razinom potrebne kontrole pristupa.
- Primijenjeno biometrijsko rješenje temelji se na senzoru otpornom na napade (kao što je upotreba digitalnog tiska za prepoznavanje otisaka prstiju).
- Broj pokušaja autentifikacije je ograničen.
- Biometrijski model pohranjuje se u vozilu u šifriranom obliku s pomoću najsuvremenijeg kriptografskog algoritma i upravljanja ključevima.
- Neobrađeni podaci koji se upotrebljavaju za izradu biometrijskog modela i autentifikaciju korisnika obrađuju se u stvarnom vremenu, a da se nikad ne pohrane, čak ni lokalno.

2.1.3. Podaci iz kojih se otkrivaju kaznena djela ili drugi prekršaji

67. Kako bi se obradili podaci koji se odnose na potencijalna kaznena djela u smislu članka 10. Opće uredbe o zaštiti podataka, Odbor preporučuje da se pribjegne lokalnoj obradi podataka nad kojom ispitanik ima potpunu kontrolu (vidjeti razmatranja o lokalnoj obradi u odjeljku 2.4.). Osim u slučaju nekih izuzeća (vidjeti studiju slučaja o studijama o nesrećama u odjeljku 3.3. u nastavku), zabranjena je vanjska obrada podataka iz kojih se otkrivaju kaznena djela ili drugi prekršaji. Stoga se, s obzirom na osjetljivost podataka, moraju uspostaviti stroge sigurnosne mjere, kao što su one opisane u odjeljku 2.7., kako bi se pružila zaštita od nezakonitog pristupa, izmjene i brisanja tih podataka.

[37] Načelo zabrane utvrđeno člankom 9. stavkom 1. Opće uredbe o zaštiti podataka odnosi se isključivo na „biometrijsk[e] podatk[e] u svrhu jedinstvene identifikacije pojedinca”.

68. Iz nekih kategorija osobnih podataka iz povezanih vozila moglo bi se otkriti da je kazneno djelo ili drugi prekršaj počinjen ili je u tijeku („podaci koji se odnose na kaznena djela”) i stoga bi one mogle biti obuhvaćene posebnim ograničenjima (npr. podaci koji pokazuju da je vozilo prešlo bijelu crtu, podaci o trenutačnoj brzini vozila u kombinaciji s preciznim podacima o lokaciji). Ako nadležna državna tijela obrađuju takve podatke u svrhu kriminalističke istrage i progona kaznenih djela, primjenjuju se zaštitne mjere predviđene člankom 10. Opće uredbe o zaštiti podataka.

2.2. Svrhe

69. Osobni podaci mogu se upotrebljavati u različite svrhe u pogledu povezanih vozila, uključujući sigurnost vozača, osiguranje, učinkovit prijevoz, usluge zabavnog ili informativnog sadržaja. U skladu s Općom uredbom o zaštiti podataka voditelji obrade podataka moraju osigurati da su njihove svrhe „posebne, izričite i zakonite”, da se ne smiju dalje obrađivati na način koji nije u skladu s tim svrhama te da postoji valjana pravna osnova za obradu u skladu s člankom 5. Opće uredbe o zaštiti podataka. Neki konkretni primjeri svrha koje voditelji obrade podataka mogu imati u kontekstu povezanih vozila razmatraju se u 3. dijelu ovih smjernica, u kojem se daju i posebne preporuke za svaku vrstu obrade.

2.3. Relevantnost i smanjenje količine podataka

70. U skladu s načelom smanjenja količine podataka[38] proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebali bi posvetiti posebnu pozornost kategorijama podataka koje su im potrebne iz povezanog vozila jer se prikupljaju isključivo osobni podaci koji su relevantni i nužni za obradu. Primjerice, podaci o lokaciji posebno su intruzivni i mogu otkriti mnoge životne navike ispitanika. U skladu s time sudionici iz industrije trebali bi biti posebno oprezni i ne bi smjeli prikupljati podatke o lokaciji, osim ako je to nužno za svrhu obrade (vidjeti prethodna razmatranja o podacima o lokaciji u odjeljku 2.1.).

2.4. Tehnička i integrirana zaštita podataka

71. Uzimajući u obzir količinu i raznolikost osobnih podataka koje proizvode povezana vozila, Odbor napominje da su voditelji obrade podataka dužni osigurati da se tehnologije primijenjene u kontekstu povezanih vozila konfiguriraju tako da se poštuje privatnost pojedinaca primjenom obaveza tehničke i integrirane zaštite podataka u skladu s člankom 25. Opće uredbe o zaštiti podataka. Tehnologije bi trebale biti dizajnirane tako da smanjuju količinu prikupljenih osobnih podataka, omogućuju zadane postavke kojima se štiti privatnost ispitanika i osiguravaju da su ispitanici dobro informirani i mogu jednostavno izmijeniti konfiguracije povezane s njihovim osobnim podacima. Konkretne smjernice o tome kako proizvođači i davatelji usluga mogu postupati u skladu s tehničkom i integriranom zaštitom podataka mogu biti korisne za industriju i treće davatelje aplikacija.

72. Neke opće prakse, opisane u nastavku, mogu pomoći i u ublažavanju rizika za prava i slobode pojedinaca u pogledu povezanih vozila[39].

2.4.1. Lokalna obrada osobnih podataka

73. Općenito, proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebali bi, kad god je to moguće, provoditi postupke koji ne uključuju osobne podatke ili prijenos osobnih podataka izvan vozila (tj. podaci se obrađuju interno). Međutim, priroda povezanih vozila donosi rizike, kao što su mogućnost napada vanjskih dionika na lokalnu obradu ili curenje lokalnih podataka uslijed prodaje dijelova vozila. Stoga bi se trebale uzeti u obzir sigurnosne mjere kako bi se osiguralo da lokalna obrada ostane lokalna i tome posvetiti odgovarajuću pozornost. Prednost je tog scenarija što nudi jamstvo da će korisnik imati isključivu i potpunu kontrolu nad vlastitim podacima, što dovodi do „tehničkog”

[38] Članak 5. stavak 1. točka (c) Opće uredbe o zaštiti podataka.
[39] Vidjeti i Europski odbor za zaštitu podataka, Smjernice 4/2019 o članku 25. – Tehnička i integrirana zaštita podataka, verzija 2.0., donesene 20. listopada 2020. (dalje u tekstu: „Smjernice 4/2019”).

smanjenja rizika u pogledu privatnosti, posebno zabranom dionicima da obrađuju bilo kakve podatke bez znanja ispitanika. Time se omogućuje i obrada osjetljivih podataka, kao što su biometrijski podaci ili podaci o kaznenim djelima ili drugim prekršajima, kao i detaljnih podataka o lokaciji koji bi inače podlijegali strožim pravilima (vidjeti u nastavku). Jednako tako, time se smanjuju rizici u području kibersigurnosti i skraćuje se razdoblje čekanja, što je posebno prikladno za automatske funkcije koje se odnose na pomoć u vožnji. Neki primjeri te vrste rješenja mogu uključivati:

- aplikacije za ekološku vožnju koje obrađuju podatke u vozilu kako bi u stvarnom vremenu na ugrađenom zaslonu prikazale savjete o ekološkoj vožnji
- aplikacije koje uključuju prijenos osobnih podataka na uređaj kao što je pametni telefon pod potpunim nadzorom korisnika (primjerice, putem Bluetootha ili Wi-Fi mreže) u slučajevima kad se podaci o vozilu ne prenose davateljima aplikacija ili proizvođačima vozila; to bi uključivalo, primjerice, spajanje pametnih telefona za upotrebu zaslona u automobilu, multimedijskih sustava, mikrofona (ili drugih senzora) za telefonske pozive itd. u mjeri u kojoj prikupljeni podaci ostaju pod kontrolom ispitanika i upotrebljavaju se isključivo za pružanje usluge koju je ispitanik zatražio
- aplikacije za poboljšanje sigurnosti u vozilu, kao što su one koje emitiraju zvučne signale ili uzrokuju vibracije upravljača pri pretjecanju automobila bez davanja znaka pokazivačem smjera ili pri prelasku bijele crte na kolniku ili kao što su one koje daju upozorenja o stanju vozila (npr. upozorenje o trošenju i habanju kočnih pločica)
- aplikacije za otključavanje, pokretanje i/ili aktiviranje određenih naredbi vozila upotrebom biometrijskih podataka vozača koji su pohranjeni u vozilu (kao što su modeli lica ili glasa ili minucije otiska prsta).

74. Aplikacije kao što su te prethodno navedene uključuju obradu podataka koju provodi pojedinac tijekom isključivo osobnih aktivnosti (tj. bez prijenosa osobnih podataka voditelju ili izvršitelju obrade podataka). Stoga, u skladu s člankom 2. stavkom 2. Opće uredbe o zaštiti podataka, **te aplikacije nisu obuhvaćene područjem primjene Opće uredbe o zaštiti podataka.**

75. Međutim, iako se ne primjenjuje na obradu osobnih podataka koju provodi pojedinac tijekom isključivo osobnih ili kućnih aktivnosti, Opća uredba o zaštiti podataka primjenjuje se na voditelje obrade ili izvršitelje obrade koji pružaju sredstva za obradu osobnih podataka za takve osobne ili kućne aktivnosti (proizvođači automobila, davatelji usluga itd.) u skladu s uvodnom izjavom 18. Opće uredbe o zaštiti podataka. Stoga, kad djeluju kao voditelji ili izvršitelji obrade podataka, moraju razviti sigurne aplikacije za upotrebu u automobilu te pritom poštovati načela tehničke i integrirane privatnosti. U svakom slučaju, u uvodnoj izjavi 78. Opće uredbe o zaštiti podataka navodi se da „[p]rilikom razvijanja, osmišljavanja, odabira i upotrebe aplikacija, usluga i proizvoda koji se temelje na obradi osobnih podataka ili obrađuju osobne podatke kako bi ispunili svoju zadaću, proizvođače proizvoda, usluga i aplikacija trebalo bi poticati da uzmu u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija i da uzimajući u obzir najnovija dostignuća osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka”[40]. S jedne će se strane poboljšati razvoj usluga usmjerenih na korisnika, a s druge olakšati i osigurati svaka daljnja upotreba u budućnosti koja bi mogla biti obuhvaćena područjem primjene Opće uredbe o zaštiti podataka. Konkretnije, Odbor preporučuje razvoj sigurne aplikacijske platforme za upotrebu u vozilu, fizički odvojene od funkcija važnih za sigurnost automobila kako pristup podacima iz automobila ne bi ovisio o nepotrebnim vanjskim kapacitetima u oblaku.

[40] Vidjeti i Smjernice 4/2019 za više preporuka o tehničkoj i integriranoj privatnosti.

76. Proizvođači automobila i davatelji usluga trebali bi, kad god je to moguće, uzeti u obzir lokalnu obradu podataka kako bi se ublažili mogući rizici od obrade u oblaku, kao što je naglašeno u mišljenju o računalstvu u oblaku koje je objavila Radna skupina iz članka 29.[41]

77. Općenito, korisnici bi trebali moći kontrolirati kako se njihovi podaci prikupljaju i obrađuju u vozilu:

- Informacije o obradi moraju se navesti na jeziku vozača (priručnik, postavke itd.).
- Odbor preporučuje da se u vozilo integrira obrada samo onih podataka koji su neophodni za funkcioniranje vozila. Ispitanici bi trebali imati mogućnost aktiviranja ili deaktiviranja obrade podataka za svaku drugu svrhu i voditelja/izvršitelja obrade te bi trebali imati mogućnost brisanja predmetnih podataka, uzimajući u obzir svrhu i pravnu osnovu obrade podataka.
- Podaci se ne bi trebali prenositi nijednoj trećoj strani (tj. korisnik je jedini koji ima pristup podacima).
- Podatke treba zadržati onoliko dugo koliko je potrebno da se pruži usluga ili koliko je propisano pravom Unije ili države članice.
- Ispitanici bi trebali moći trajno izbrisati sve osobne podatke prije nego što se vozila stave na prodaju.
- Ako je izvedivo, ispitanici bi trebali imati izravan pristup podacima koje proizvode te aplikacije.

78. Naposljetku, iako možda nije uvijek moguće pribjeći lokalnoj obradi podataka za svaki slučaj upotrebe, često se može uspostaviti „hibridna obrada”. Na primjer, u kontekstu osiguranja utemeljenog na upotrebi osobni podaci o ponašanju u vožnji (kao što je sila primijenjena na papučicu kočnice, broj prijeđenih kilometara itd.) mogu se obrađivati u vozilu ili ih obrađuje davatelj telematičkih usluga u ime društva za osiguranje (voditelj obrade podataka) kako bi dodijelio brojčane ocjene koje se prenose društvu za osiguranje na utvrđenoj osnovi (npr. svaki mjesec). Na taj način društva za osiguranje ne dobivaju pristup neobrađenim podacima o ponašanju, već samo agregiranoj ocjeni nakon obrade. Time se osigurava tehničko ispunjavanje načela smanjenja količine podataka. To znači i da korisnici moraju imati mogućnost ostvarivanja svojeg prava kad druge strane pohranjuju podatke: primjerice, korisnik bi trebao imati mogućnost brisanja podataka koji su pohranjeni u sustavima automehaničarske radionice ili prodavaonice automobila u skladu s uvjetima iz članka 17. Opće uredbe o zaštiti podataka.

2.4.2. Anonimizacija i pseudonimizacija

79. Ako je predviđen prijenos osobnih podataka izvan vozila, prije prijenosa trebalo bi razmotriti njihovu anonimizaciju. Pri anonimizaciji bi voditelj obrade trebao uzeti u obzir svu obuhvaćenu obradu koja bi potencijalno mogla dovesti do ponovne identifikacije podataka, kao što je prijenos lokalno anonimiziranih podataka. Odbor podsjeća na to da se načela zaštite podataka ne primjenjuju na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ili na osobne podatke koji su anonimizirani tako da se identitet ispitanika ne može ili više ne može utvrditi[42]. Kad je skup podataka zaista anonimiziran i više se ne može utvrditi identitet pojedinaca, više se ne primjenjuje europsko pravo o zaštiti podataka. Anonimizacija stoga može biti dobra strategija kojom se prema potrebi zadržavaju koristi i ublažavaju rizici koji se odnose na povezana vozila.

[41] Radna skupina iz članka 29., Mišljenje 5/2012 o računalstvu u oblaku: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
[42] Vidjeti članak 4. točku 1. i uvodnu izjavu 26. Opće uredbe o zaštiti podataka.

80. Kako bi se postigla anonimizacija podataka, mogu se upotrebljavati razne metode, a ponekad i njihova kombinacija, kao što je detaljno navedeno u mišljenju Radne skupine iz članka 29. o tehnikama anonimizacije[43].

81. Druge tehnike kao što je pseudonimizacija[44] mogu pomoći u ublažavanju rizika koji proizlaze iz obrade podataka, uzimajući u obzir da u većini slučajeva podaci iz kojih se može izravno utvrditi identitet nisu nužni za postizanje svrhe obrade. Ako je ojačana sigurnosnim zaštitnim mjerama, pseudonimizacija poboljšava zaštitu osobnih podataka smanjivanjem rizika od zloupotrebe. Za razliku od anonimizacije, pseudonimizacija je reverzibilna, a pseudonimizirani podaci smatraju se osobnim podacima koji su obuhvaćeni Općom uredbom o zaštiti podataka.

2.4.3. Procjene učinka na zaštitu podataka

82. S obzirom na opseg i osjetljivost osobnih podataka koje mogu proizvesti povezana vozila vjerojatno je da će obrada, posebno ako se osobni podaci obrađuju izvan vozila, često dovesti do visokog rizika za prava i slobode pojedinaca. U tom su slučaju sudionici u industriji dužni obaviti procjenu učinka na zaštitu podataka (DPIA) kako bi se utvrdili i ublažili rizici, kako je detaljno obrazloženo u člancima 35. i 36. Opće uredbe o zaštiti podataka. Čak i onda kad procjena učinka nije potrebna, bilo bi najbolje provesti je što prije u postupku dizajniranja. To će omogućiti sudionicima u industriji da rezultate te analize uzmu u obzir u odlukama o dizajnu prije uvođenja novih tehnologija.

2.5. Informiranje

83. Prije obrade osobnih podataka ispitanika treba obavijestiti o identitetu voditelja obrade podataka (npr. proizvođač vozila i opreme ili davatelj usluga), svrsi obrade, primateljima podataka, razdoblju pohrane podataka i pravima ispitanika u skladu s Općom uredbom o zaštiti podataka[45].

84. Proizvođač vozila i opreme, davatelj usluga ili drugi voditelj obrade podataka trebao bi ispitaniku dostaviti i sljedeće informacije u jasnom, jednostavnom i lako dostupnom obliku:

- kontaktne podatke službenika za zaštitu podataka
- svrhe obrade radi kojih se upotrebljavaju osobni podaci i pravnu osnovu za obradu
- izričito navođenje legitimnih interesa voditelja obrade podataka ili treće strane kad takvi legitimni interesi čine pravnu osnovu za obradu
- primatelje ili kategorije primatelja osobnih podataka prema potrebi
- razdoblje u kojem će se osobni podaci pohranjivati ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje
- postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade podataka koji se odnose na ispitanika te postojanje prava na ulaganje prigovora na obradu, kao i prava na prenosivost podataka
- postojanje prava da se u bilo kojem trenutku privola povuče, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena

[43] Radna skupina iz članka 29., Mišljenje 05/2014 o tehnikama anonimizacije: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hr.pdf
[44] Članak 4. točka 5. Opće uredbe o zaštiti podataka. Izvješće ENISA-e od 3. prosinca 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] Članak 5. stavak 1. točka (a) i članak 13. Opće uredbe o zaštiti podataka. Vidjeti i Smjernice o transparentnosti na temelju Uredbe 2016/679 Radne skupine iz članka 29. (wp260rev.01), koje je odobrio Odbor.

- ako je primjenjivo, činjenicu da voditelj obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji i zaštitne mjere koje se upotrebljavaju za njihov prijenos
- informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili zahtjev nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže
- postojanje automatiziranog donošenja odluka, što uključuje izradu profila koja proizvodi pravne učinke koji se odnose na ispitanika ili na sličan način značajno na njega utječu te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika; to bi posebno mogao biti slučaj ako se usluge osiguranja utemeljenog na upotrebi pružaju pojedincima
- pravo na podnošenje prigovora nadzornom tijelu
- informacije o daljnjoj obradi
- u slučaju zajedničkog vođenja obrade podataka jasne i potpune informacije o odgovornostima svakog voditelja obrade podataka.

85. U nekim se slučajevima osobni podaci ne prikupljaju izravno od predmetnog pojedinca. Primjerice, proizvođač vozila i opreme može se osloniti na prodavača koji će prikupiti informacije o vlasniku vozila kako bi ponudio uslugu hitne pomoći na cesti. Kad podaci nisu prikupljeni izravno, proizvođač vozila i opreme, davatelj usluga ili drugi voditelj obrade podataka, trebao bi navesti, uz prethodne informacije, i kategorije osobnih podataka o kojima je riječ, izvor osobnih podataka i, ako je primjenjivo, informaciju o tome dolaze li podaci iz javno dostupnih izvora. Voditelj obrade mora dostaviti te informacije u razumnom roku nakon dobivanja podataka, a **najkasnije do prvog od sljedećih datuma** u skladu s člankom 14. stavkom 3. Opće uredbe o zaštiti podataka: i. u roku od mjesec dana nakon dobivanja osobnih podataka, uzimajući u obzir posebne okolnosti obrade osobnih podataka, ii. u trenutku prve komunikacije ostvarene s ispitanikom ili iii. prije prijenosa podataka ako se ti podaci prenose trećoj strani.

86. Ispitanicima će se možda trebati dostaviti nove informacije ako za njih postane odgovoran novi voditelj obrade podataka. Ovisno o zemlji ili regiji u kojoj je potrebna pomoć, uslugu pomoći na cesti koja omogućuje interakciju s povezanim vozilima mogu pružiti različiti voditelji obrade podataka. Novi voditelji obrade podataka trebali bi ispitanicima dostaviti potrebne informacije kad oni prelaze granice, a usluge koje omogućuju interakciju s povezanim vozilima pružaju novi voditelji obrade podataka.

87. Informacije upućene ispitanicima mogu se dostaviti na dvjema razinama[46], tj. mogu se podijeliti na informacije koje su najvažnije za ispitanike (prva razina) i informacije koje bi kasnije mogle biti od interesa za njih (druga razina). Osim identiteta voditelja obrade podataka, prvorazinske informacije uključuju svrhu obrade i opis prava ispitanika, kao i sve dodatne informacije o obradi koja najviše utječe na ispitanika i obradi koja bi ga mogla iznenaditi. Odbor preporučuje da bi, u kontekstu povezanih vozila, ispitanika trebalo obavijestiti o svim primateljima na prvoj razini informacija. Kako je navedeno u smjernicama o transparentnosti Radne skupine iz članka 29., voditelji obrade trebali bi dostaviti informacije o primateljima koje imaju najviše smisla za ispitanike. U praksi će to biti imenovani primatelji kako bi ispitanici točno znali tko ima njihove osobne podatke. Ako voditelji obrade ne mogu dostaviti imena primatelja, informacije bi trebale biti što konkretnije tako da se u njima navede vrsta primatelja (tj. upućivanjem na aktivnosti koje provodi), industrija, sektor i podsektor te lokacija primateljâ.

[46] Vidjeti Smjernice o transparentnosti na temelju Uredbe 2016/679 Radne skupine iz članka 29.(wp260rev.01), koje je odobrio Odbor.

88. Informacije o tome mogu se ispitanicima dostaviti u obliku sažetih i lako razumljivih klauzula u ugovoru o kupoprodaji vozila ili pružanju usluga i/ili bilo kojim sredstvom pisane komunikacije, upotrebom posebnih dokumenata (npr. servisna knjižnica ili priručnik za održavanje vozila) ili s pomoću računala u vozilu.

89. U skladu s člankom 13. i člankom 14. Opće uredbe o zaštiti podataka nužne informacije mogu biti popraćene standardiziranim ikonama kako bi se transparentnost povećala potencijalnim smanjenjem potrebe da se ispitaniku prikazuje velika količina pisanih informacija. Trebale bi biti vidljive u vozilu kako bi se na razumljiv i jasno čitljiv način pružio smislen pregled namjeravane obrade. Odbor naglašava važnost standardizacije tih ikona kako bi korisnik mogao pronaći iste simbole neovisno o marki ili modelu vozila. Primjerice, kad se prikupljaju određene vrste podataka, na primjer podaci o lokaciji, u vozilu bi se trebao prikazati jasan signal (kao što je svjetlo unutar vozila) koji bi obavijestio putnike o prikupljanju podataka.

2.6. Prava ispitanika

90. Proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebali bi ispitanicima olakšati kontrolu nad njihovim podacima tijekom cijelog razdoblja obrade primjenom posebnih alata kojima se pruža učinkovit način za ostvarivanje njihovih prava, posebno prava na pristup, ispravak, brisanje, njihova prava na ograničenje obrade i, ovisno o pravnoj osnovi za obradu, prava na prenosivost podataka i prava na prigovor.

91. Radi lakše izmjene postavki trebalo bi uspostaviti sustav upravljanja profilima kako bi se pohranile postavke poznatih vozača i kako bi im se pomoglo da u bilo kojem trenutku na jednostavan način promijene svoje postavke privatnosti. Sustav upravljanja profilima trebao bi centralizirati svaku postavku podataka za svaku obradu podataka, posebno kako bi se olakšao pristup, brisanje, uklanjanje i prenosivost osobnih podataka iz sustavâ vozila na zahtjev ispitanika. Vozačima bi trebalo omogućiti da u bilo kojem trenutku privremeno ili trajno zaustave prikupljanje određenih vrsta podataka, osim ako postoji posebna pravna osnova na koju se voditelj obrade može pozvati kako bi nastavio prikupljati posebne podatke. Kad je riječ o ugovoru u kojem se nudi personalizirana ponuda utemeljena na ponašanju u vožnji standardni uvjeti tog ugovora trebali bi se ponovno primjenjivati na korisnika. Te bi se značajke trebale primijeniti unutar vozila iako bi se ispitanicima mogle pružiti i dodatnim sredstvima (npr. namjenske aplikacije). Nadalje, Odbor preporučuje proizvođačima da osiguraju jednostavnu funkciju (kao što je gumb za brisanje) kako bi se ispitanicima omogućilo brzo i jednostavno uklanjanje osobnih podataka koji se mogu pohraniti na upravljačkoj ploči automobila (primjerice, povijest GPS navigacije, pretraživanje interneta itd.).

92. Prodaja povezanog vozila i posljedična promjena vlasništva isto bi tako trebale potaknuti brisanje svih osobnih podataka koji više nisu nužni za prethodno navedene svrhe, a ispitanik bi trebao imati mogućnost ostvarivanja svojeg prava na prenosivost.

2.7. Sigurnost

93. Proizvođači vozila i opreme, davatelji usluga i drugi voditelji obrade podataka trebali bi uvesti mjere kojima se jamči sigurnost i povjerljivost obrađenih podataka i poduzeti odgovarajuće mjere opreza kako bi spriječili da neovlaštene osobe preuzmu kontrolu. Sudionici u industriji posebno bi trebali razmotriti uvođenje sljedećih mjera:

- šifriranje komunikacijskih kanala upotrebom najsuvremenijeg algoritma
- uspostavljanje sustava upravljanja kriptografskim ključevima koji je jedinstven za svako vozilo, a ne za svaki model
- šifriranje podataka upotrebom najsuvremenijeg algoritma kad se podaci pohranjuju na daljinu

- redovita obnova kriptografskih ključeva
- zaštita kriptografskih ključeva od otkrivanja
- autentifikacija uređaja za primanje podataka
- osiguranje cjelovitosti podataka (npr. raspršivanjem)
- omogućavanje ispitanicima da pristupe pouzdanim tehnikama autentifikacije korisnika (lozinka, elektronički certifikat itd.).

94. Konkretnije, Odbor preporučuje da proizvođači vozila provode sljedeće sigurnosne mjere:

- razdvajanje ključnih funkcija vozila od onih koje se uvijek oslanjanju na telekomunikacijske kapacitete (npr. sustava za informativni i zabavni sadržaj)
- primjena tehničkih mjera koje proizvođačima vozila omogućuju da brže isprave sigurnosne ranjivosti tijekom cijelog životnog vijeka vozila
- davanje što veće prednosti, kad je riječ o ključnim funkcijama vozila, upotrebi sigurnih sredstava komunikacije koja su posebno namijenjena prijevozu
- uspostavljanje alarmnog sustava u slučaju napada na sustave vozila koji nudi mogućnost degradiranog načina rada[47]
- pohrana evidencije svakog pristupa informacijskom sustavu vozila, pri čemu je npr. šest mjeseci najdulje razdoblje pohrane, kako bi se omogućilo otkrivanje izvora potencijalnog napada i povremeno pregledale evidentirane informacije radi otkrivanja mogućih nepravilnosti.

95. Te bi se opće preporuke trebale dopuniti posebnim zahtjevima uzimajući u obzir značajke i svrhu svake obrade podataka.

2.8. Prijenos osobnih podataka trećim stranama

96. Načelno samo voditelj obrade podataka i ispitanik imaju pristup podacima koje proizvode povezana vozila. Međutim, voditelj obrade podataka može prenijeti osobne podatke komercijalnom partneru (primatelju) u mjeri u kojoj se takav prijenos zakonito poziva na jednu od pravnih osnova iz članka 6. Opće uredbe o zaštiti podataka.

97. S obzirom na moguću osjetljivost podataka o upotrebi vozila (npr. obavljena putovanja, način vožnje) Odbor preporučuje sustavno dobivanje pristanka/privole ispitanika prije nego što se njegovi podaci prenesu komercijalnom partneru koji djeluje kao voditelj obrade podataka (primjerice, označivanjem kućice koja nije prethodno označena ili, kad je to tehnički moguće, upotrebom fizičkog ili logičkog uređaja kojem osoba može pristupiti iz vozila). Komercijalni partner postaje odgovoran za podatke koje prima i podliježe svim odredbama Opće uredbe o zaštiti podataka.

98. Proizvođač vozila, davatelj usluga ili drugi voditelj obrade podataka mogu prenositi osobne podatke izvršitelju obrade podataka odabranom da sudjeluje u pružanju usluge ispitaniku, pod uvjetom da izvršitelj obrade ne upotrebljava te podatke za vlastite svrhe. Voditelji ili izvršitelji obrade podataka trebali bi sastaviti ugovor ili drugi pravni dokument u kojem se navode obaveze svake stranke i prenose odredbe članka 28. Opće uredbe o zaštiti podataka.

2.9. Prijenos osobnih podataka izvan EU-a/EGP-a

[47] Degradirani način rada je način rada vozila kojim se jamči rad funkcija nužnih za siguran rad vozila (tj. minimalni sigurnosni zahtjevi), čak i ako bi se deaktivirale druge manje važne funkcije (npr. rad uređaja za navigaciju ne smatra se ključnim, za razliku od rada kočnog sustava).

99. U slučaju prijenosa osobnih podataka izvan Europskog gospodarskog prostora predviđene su posebne zaštitne mjere kako bi se osiguralo da podaci budu zaštićeni tijekom prijenosa.

100. To znači da voditelj obrade podataka može prenijeti osobne podatke primatelju samo u mjeri u kojoj je takav prijenos u skladu sa zahtjevima utvrđenima u poglavlju V. Opće uredbe o zaštiti podataka.

2.10. Upotreba Wi-Fi tehnologija u vozilima

101. Zahvaljujući dostignućima u mobilnoj tehnologiji internet se može bez problema upotrebljavati tijekom vožnje. Iako se u vozilu mogućnost povezivanja s Wi-Fi mrežom može osigurati putem pristupnih točaka pametnog telefona ili za to predviđenih uređaja (hardverski ključ s OBD-II priključkom, bežični modem ili usmjerivač itd.), većina današnjih proizvođača nudi modele koji uključuju ugrađenu mobilnu podatkovnu vezu i koji mogu stvoriti Wi-Fi mreže. Ovisno o slučaju, moraju se uzeti u obzir različiti aspekti:

ZProfesionalni cestovni prijevoznici, kao što su vozači taksija, mogu svojim klijentima ponuditi uslugu povezivanja s Wi-Fi mrežom. U tom se slučaju profesionalac ili njegovo poduzeće mogu smatrati davateljima internetskih usluga (ISP) i stoga podliježu posebnim obvezama i ograničenjima u pogledu obrade osobnih podataka svojih klijenata.

ZMogućnost povezivanja s Wi-Fi mrežom ugrađuje se isključivo za potrebe vozača (isključujući vozača i njegove putnike). U tom se slučaju obrada osobnih podataka smatra isključivo osobnom ili kućnom aktivnošću u skladu s člankom 2. stavkom 2. točkom (c) i uvodnom izjavom 18. Opće uredbe o zaštiti podataka.

102. Općenito, porast broja sučelja za povezivanje na internet putem Wi-Fi mreže čini sve veći rizik za privatnost pojedinaca. Korisnici putem vlastitih vozila neprekidno emitiraju podatke i stoga ih se može pratiti i identificirati. Kako bi se spriječilo praćenje, proizvođači vozila i opreme trebali bi stoga ponuditi korisniku mogućnost da odbije prikupljanje naziva Wi-Fi mreže (SSID) koja se upotrebljava u vozilu.

3. STUDIJE SLUČAJA

103. Ovaj se odjeljak odnosi na pet konkretnih primjera obrade u kontekstu povezanih vozila koji odgovaraju scenarijima u kojima bi se dionici u sektoru lako mogli naći. Primjeri obuhvaćaju obradu podataka u kojoj se mora izračunati snaga koja se ne može mobilizirati lokalno u vozilu i/ili se osobni podaci moraju poslati trećoj strani radi daljnje analize ili daljinskog omogućavanja dodatne funkcije. Za svaku vrstu obrade u ovom se dokumentu navode predviđene svrhe, kategorije prikupljenih podataka, razdoblje zadržavanja takvih podataka, prava ispitanika, sigurnosne mjere koje je potrebno provesti i primatelji informacija. Ako neke od tih kategorija nisu opisane u nastavku, primjenjuju se opće preporuke opisane u prethodnom dijelu.

104. Odabrani primjeri nisu potpuni, no ukazuju na razne vrste obrade, pravne osnove, dionike itd. koji bi se mogli pojaviti u kontekstu povezanih vozila.

3.1. Usluga koju pruža treća strana

105. Ispitanici mogu sklopiti ugovor s davateljem usluga kako bi dobili usluge s dodanom vrijednosti u pogledu svojeg vozila. Primjerice, ispitanik može sklopiti ugovor o osiguranju utemeljen na upotrebi u kojem se nude niže premije osiguranja za osobe koje rjeđe voze („plati koliko voziš”) odnosno koje se odgovorno ponašaju u vožnji („plati kako voziš”) i zbog kojeg društva za osiguranje moraju pratiti vozačke navike. Ispitanik bi mogao sklopiti ugovor i s poduzećem koje nudi pomoć na cesti u slučaju kvara i kojem se stoga moraju prenijeti podaci o lokaciji vozila ili s davateljem usluga radi primanja poruka ili upozorenja o radu vozila (npr. upozorenje o istrošenosti kočnica ili podsjetnik na datum tehničkog pregleda).

3.1.1. Osiguranje utemeljeno na upotrebi

106. „Plati koliko voziš” je vrsta osiguranja utemeljenog na upotrebi u okviru kojeg se prati broj prijeđenih kilometara i/ili vozačke navike kako bi se utvrdilo koji su vozači „sigurni” tako da ih se nagradi nižim premijama. Osiguravatelj će zahtijevati od vozača da instalira ugrađenu telematičku uslugu, mobilnu aplikaciju ili da aktivira modul ugrađen pri proizvodnji koji prati

prijeđene kilometre i/ili ponašanje u vožnji (načini kočenja, veliko ubrzanje itd.). Podaci prikupljeni telematičkim uređajem upotrebljavat će se za dodjelu ocjena vozaču kako bi se analiziralo koje rizike može činiti za društvo za osiguranje.

107. Budući da je člankom 5. stavkom 3. Direktive o e-privatnosti utvrđeno da je u slučaju osiguranja utemeljenog na upotrebi obvezan pristanak, Odbor ističe da ugovaratelj osiguranja mora imati mogućnost ugovaranja police osiguranja koje nije utemeljeno na upotrebi. U suprotnom bi se smatralo da se pristanak nije dao dobrovoljno jer bi izvršenje ugovora ovisilo o davanju pristanka. Nadalje, člankom 7. stavkom 3. Opće uredbe o zaštiti podataka utvrđeno je da ispitanici imaju pravo na povlačenje privole.

3.1.1.1. Pravna osnova

108. Kad se podaci prikupljaju putem javno dostupne elektroničke komunikacijske usluge (primjerice, SIM kartica koja se nalazi u telematičkom uređaju), bit će potreban pristanak kako bi se pristupilo informacijama koje su već pohranjene u vozilu kako je propisano člankom 5. stavkom 3. Direktive o e-privatnosti. Nijedno izuzeće predviđeno tim odredbama ne može se primijeniti u tom kontekstu: obrada se ne odvija isključivo u svrhu prijenosa komunikacije putem elektroničke komunikacijske mreže niti se odnosi na neku uslugu informacijskog društva koju je pretplatnik ili korisnik izričito zatražio. Pristanak bi se mogao pribaviti u trenutku sklapanja ugovora.

109. Kad je riječ o obradi osobnih podataka nakon pohrane ili pristupa terminalnoj opremi krajnjeg korisnika, društvo za osiguranje može se u tom posebnom kontekstu pozvati na članak 6. stavak 1. točku (b) Opće uredbe o zaštiti podataka, pod uvjetom da može dokazati da se obrada provodi na temelju valjanog ugovora s ispitanikom i da je nužna kako bi se izvršio taj ugovor. Ako je obrada objektivno nužna za izvršenje ugovora s ispitanikom, Odbor smatra da u tom slučaju pozivanje na članak 6. stavak 1. točku (b) Opće uredbe o zaštiti podataka ne bi dovelo do smanjenja dodatne zaštite predviđene člankom 5. stavkom 3. Direktive o e-privatnosti. Pravna osnova ostvaruje se kad ispitanik potpiše ugovor s društvom za osiguranje.

3.1.1.2. Prikupljeni podaci

110. Dvije su vrste osobnih podataka koje treba uzeti u obzir:

- **komercijalni i transakcijski podaci**: identifikacijski podaci ispitanika, podaci o transakciji, sredstvima plaćanja itd.
- **podaci o upotrebi**: osobni podaci koje proizvodi vozilo, vozačke navike, lokacija itd.

111. Budući da postoji rizik od toga da bi se podaci prikupljeni telematičkom kutijom mogli zloupotrijebiti za izradu preciznog profila vozačevih kretanja, Odbor preporučuje sljedeće u pogledu obrade neobrađenih podataka o ponašanju u vožnji:

- treba ih obrađivati unutar vozila u telematičkim kutijama ili u korisnikovu pametnom telefonu tako da osiguravatelj ima pristup samo rezultatima (npr. ocjena vozačevih navika), a ne detaljnim neobrađenim podacima (vidjeti odjeljak 2.1.)
- ili ih treba obrađivati davatelj telematičkih usluga u ime voditelja obrade (društvo za osiguranje) kako bi dodijelio brojčane ocjene koje se na utvrđenoj osnovi prenose društvu za osiguranje. U tom slučaju neobrađeni podaci moraju se odvojiti od podataka koji su izravno povezani s identitetom vozača. To znači da davatelj telematičkih usluga prima podatke u stvarnom vremenu, ali ne zna imena, broj registarskih pločica itd. ugovaratelja osiguranja. Međutim, osiguravatelj zna imena ugovaratelja osiguranja i prima samo ocjene i ukupan broj prijeđenih kilometara, a ne neobrađene podatke na temelju kojih se dodjeljuju te ocjene.

112. Nadalje, treba napomenuti da se podaci o lokaciji ne bi trebali prikupljati ako je za izvršenje ugovora nužan samo broj prijeđenih kilometara.

3.1.1.3. Razdoblje zadržavanja

113. U kontekstu obrade podataka koja se provodi radi izvršenja ugovora (tj. pružanja usluge) važno je razlikovati dvije vrste podataka prije utvrđivanja predmetnog razdoblja zadržavanja:

- **komercijalni i transakcijski podaci:** ti se podaci mogu zadržati u aktivnoj bazi podataka tijekom cijelog trajanja ugovora, a po isteku ugovora mogu se arhivirati na fizičkoj (na posebnom mediju: DVD itd.) ili logičkoj razini (upravljanjem ovlašćivanjem) u slučaju mogućeg sudskog postupka; po isteku roka zastare podaci se brišu ili anonimiziraju

- **podaci o upotrebi:** podaci o upotrebi mogu se kvalificirati kao neobrađeni podaci i agregirani podaci. Kao što je prethodno navedeno, voditelji ili izvršitelji obrade podataka ne bi trebali obrađivati neobrađene podatke. Ako je to nužno, neobrađene podatke trebalo bi čuvati onoliko dugo koliko je potrebno da se agregirani podaci protumače i provjeri valjanost agregiranja. Agregirane podatke treba čuvati onoliko dugo koliko je potrebno da se pruži usluga ili koliko je propisano pravom Unije ili države članice.

3.1.1.4. Informiranje i prava ispitanika

114. Prije obrade osobnih podataka ispitaniku treba dostaviti informacije na transparentan i razumljiv način u skladu s člankom 13. Opće uredbe o zaštiti podataka. Posebno bi ga trebalo obavijestiti o razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje. U potonjem slučaju Odbor preporučuje primjenu pedagoškog pristupa kako bi se naglasila razlika između neobrađenih podataka i ocjene dodijeljene na temelju njih te naglašava da će u tom slučaju osiguravatelj prikupljati ocjenu samo prema potrebi.

115. Ako se podaci ne obrađuju u vozilu, već ih obrađuje davatelj telematičkih usluga u ime voditelja obrade (društvo za osiguranje), bilo bi korisno u tim informacijama navesti da u tom slučaju davatelj nema pristup podacima koji su izravno povezani s identitetom vozača (kao što su imena, brojevi registarskih pločica itd.). S obzirom na to da je važno ispitanike obavijestiti o posljedicama obrade njihovih osobnih podataka, kao i na to da ih ne bi trebala iznenaditi njihova obrada, Odbor preporučuje da bi ispitanike trebalo obavijestiti o izradi profila i posljedicama takve izrade, čak i ako ne uključuje automatizirano donošenje odluka iz članka 22. Opće uredbe o zaštiti podataka.

116. Kad je riječ o pravima ispitanika, treba ih konkretno obavijestiti o sredstvima koja su dostupna za ostvarivanje njihovih prava na pristup, ispravak, ograničenje i brisanje. Budući da se u tom kontekstu neobrađeni podaci prikupljaju od ispitanika (na određenim obrascima ili njegovom aktivnošću) i obrađuju u skladu s člankom 6. stavkom 1. točkom (b) Opće uredbe o zaštiti podataka (izvršenje ugovora), ispitanik ima pravo ostvariti svoje pravo na prenosivost podataka. Kao što je naglašeno u smjernicama o pravu na prenosivost podataka, Odbor posebno preporučuje „da voditelji obrade jasno objasne razliku između vrsta podataka koje ispitanik može primiti na temelju prava na pristup ispitanika i prava na prenosivost podataka”.[48]

117. Informacije se mogu dostaviti nakon potpisivanja ugovora.

3.1.1.5. Primatelj:

118. Odbor preporučuje da bi podatke o upotrebi vozila, koliko je to moguće, trebalo obrađivati izravno u telematičkim kutijama kako bi osiguravatelj mogao pristupiti samo podacima o rezultatima (npr. ocjena), a ne detaljnim neobrađenim podacima.

[48] Radna skupina iz članka 29., Smjernice o pravu na prenosivost podataka na temelju Uredbe 2016/676, WP242 rev.01, koje je odobrio Odbor, str. 13.

119. Ako prikuplja podatke u ime voditelja obrade (društvo za osiguranje) kako bi dodijelio brojčane ocjene, davatelj telematičke usluge ne mora znati identitet vozača (kao što su imena, brojevi registarskih pločica itd.) ugovarateljâ osiguranja.

3.1.1.6. Sigurnost:

120. Primjenjuju se opće preporuke. Vidjeti odjeljak 2.7.

3.1.2. Iznajmljivanje i rezervacija parkirnog mjesta

121. Vlasnik parkirnog mjesta možda ga želi iznajmiti. U tu svrhu navodi značajke parkirnog mjesta i njegovu cijenu u internetsku aplikaciju. Kad se prikaže oglas za parkirno mjesto, aplikacija obavještava vlasnika kad ga vozač želi rezervirati. Vozač može odabrati odredište i na temelju više kriterija provjeriti dostupnost parkirnih mjesta. Transakcija se potvrđuje nakon odobrenja vlasnika i davatelj usluge obavlja platnu transakciju, nakon čega se koristi navigacijom kako bi stigao do lokacije.

3.1.2.1. Pravna osnova

122. Kad se podaci prikupljaju putem javno dostupne elektroničke komunikacijske usluge, primjenjuje se članak 5. stavak 3. Direktive o e-privatnosti.

123. Budući da je to usluga informacijskog društva, člankom 5. stavkom 3. Direktive o e-privatnosti ne zahtijeva se pristanak za pristup informacijama koje su već pohranjene u vozilu u slučaju kad pretplatnik ili korisnik izričito zatraži takvu uslugu.

124. Članak 6. stavak 1. točka (b) čini pravnu osnovu za obradu osobnih podataka samo za podatke nužne za izvršenje ugovora kojem je ispitanik stranka.

3.1.2.2. Prikupljeni podaci

125. Obrađeni podaci uključuju vozačeve kontaktne podatke (ime, e-pošta, telefonski broj), tip vozila (npr. automobil, kamion, motocikl), broj registarske pločice, razdoblje parkiranja, pojedinosti o plaćanju (npr. podaci s kreditne kartice) i navigacijske podatke.

3.1.2.3. Razdoblje zadržavanja

126. Podaci bi se trebali zadržavati onoliko dugo koliko je nužno da se ispuni ugovor o parkiranju ili ako je drukčije predviđeno pravom Unije ili države članice. Nakon toga podaci se brišu ili anonimiziraju.

3.1.2.4. Informiranje i prava ispitanika

127. Prije obrade osobnih podataka ispitanika bi o tome trebalo obavijestiti na transparentan i razumljiv način u skladu s člankom 13. Opće uredbe o zaštiti podataka."

128. Ispitanika bi trebalo konkretno obavijestiti o sredstvima koja su dostupna za ostvarivanje njegovih prava na pristup, ispravak, ograničenje i brisanje. Budući da se u tom kontekstu podaci prikupljaju od ispitanika (na određenim obrascima ili njegovom aktivnošću) i obrađuju u skladu s člankom 6. stavkom 1. točkom (b) Opće uredbe o zaštiti podataka (izvršenje ugovora), ispitanik ima pravo ostvariti svoje pravo na prenosivost podataka. Kao što je naglašeno u smjernicama o pravu na prenosivost podataka, Odbor posebno preporučuje „da voditelji obrade jasno objasne razliku između vrsta podataka koje ispitanik može primiti na temelju prava na pristup ispitanika i prava na prenosivost podataka”.

3.1.2.5. Primatelj:

129. Načelno samo voditelj i izvršitelj obrade podataka imaju pristup podacima.

3.1.2.6. Sigurnost:

130. Primjenjuju se opće preporuke. Vidjeti odjeljak 2.7.

3.2. Sustav eCall

131. U slučaju teške nesreće u Europskoj uniji vozilo automatski aktivira poziv sustava eCall na jedinstveni europski broj za hitne službe 112 (vidjeti odjeljak 1.1. za više detalja), što

omogućuje da se hitna pomoć odmah pošalje na mjesto nesreće u skladu s Uredbom (EU) 2015/758 od 29. travnja 2015. o zahtjevima za homologaciju za uvođenje sustava eCall ugrađenog u vozilo koji se temelji na službi 112 te o izmjeni Direktive 2007/46/EZ (dalje u tekstu: „Uredba (EU) 2015/758").

132. Generator poziva sustava eCall ugrađen u vozilo, koji omogućuje prijenos putem javne mobilne bežične komunikacijske mreže, upućuje hitni poziv koji samo u slučaju nesreće automatski aktiviraju senzori u vozilu ili ručno putnici. U slučaju nesreće se osim audiokanala automatski aktivira i generiranje minimalnog skupa podataka (MSD) koji se šalje pristupnoj točki sigurnosnog poziva (PSAP).

3.2.1. Pravna osnova

133. Kad je riječ o primjeni Direktive o e-privatnosti, potrebno je uzeti u obzir dvije odredbe:

- članak 9. o podacima o lokaciji koji nisu podaci o prometu, koji se odnosi samo na elektroničke komunikacijske usluge
- članak 5. stavak 3. o pristupu informacijama pohranjenima na generatoru ugrađenom u vozilu.

134. Iako je u načelu tim odredbama propisan obvezan pristanak ispitanika, Uredba (EU) 2015/758 pravno je obvezujuća za voditelja obrade podataka (ispitanik zapravo nema slobodu ni mogućnost da odbije obradu svojih podataka). Stoga Uredba (EU) 2015/758 nadjačava potrebu za dobivanjem vozačeva pristanka za obradu osobnih podataka i MSD-a[49].

135. Pravna osnova za obradu tih podataka bit će poštovanje pravnih obveza kako je predviđeno u članku 6. stavku 1. točki (c) Opće uredbe o zaštiti podataka (tj. poštovanje Uredbe (EU) 2015/758).

3.2.2. Prikupljeni podaci

136. Uredbom (EU) 2015/758 utvrđeno je da podaci koje šalje sustav eCall ugrađen u vozilo koji se temelji na službi 112 uključuju samo minimalne informacije, kako je navedeno u normi EN 15722:2015 „Inteligentni transportni sustavi – Elektronička sigurnost – Najmanji skup podataka za elektroničke hitne pozive iz vozila (MSD)", a to su:

- naznaka o tome je li poziv sustava eCall aktiviran ručno ili automatski
- tip vozila
- identifikacijski broj vozila (VIN)
- tip pogona vozila
- vremenska oznaka prve podatkovne poruke generirane pri aktualnom incidentu povezanom s pozivom sustava eCall
- posljednja poznata zemljopisna širina i dužina položaja vozila utvrđene u najkasnijem mogućem trenutku prije generiranja poruke
- posljednji poznati stvarni smjer putovanja utvrđen u najkasnijem mogućem trenutku prije generiranja poruke (samo posljednje tri lokacije vozila).

[49] Treba napomenuti da se u članku 8. stavku 1. točki (f) pregovaračkog mandata Vijeća za prijedlog uredbe o „e-privatnosti" predviđa posebno izuzeće za sustav eCall jer pristanak nije potreban kad „treba utvrditi lokaciju terminalne opreme u slučajevima kad krajnji korisnik uspostavi komunikaciju u slučaju opasnosti s hitnim službama putem jedinstvenog europskog broja za hitne službe 112 ili nacionalnog broja za hitne službe u skladu s člankom 13. stavkom 3."

3.2.3. Razdoblje zadržavanja

137. Uredbom (EU) 2015/758 propisano je da se podaci ne zadržavaju dulje nego što je potrebno u svrhu rješavanja izvanrednih situacija. Takvi podaci potpuno se brišu čim više nisu potrebni za tu svrhu. Nadalje, podaci se automatski i neprestano brišu u unutarnjoj memoriji sustava eCall. Dopušteno je zadržavanje samo posljednjih triju lokacija vozila u mjeri u kojoj je to strogo nužno za određivanje trenutačne lokacije vozila i smjera putovanja u vrijeme događaja.

3.2.4. Informiranje i prava ispitanika

138. Člankom 6. Uredbe (EU) 2015/758 utvrđeno je da proizvođači dostavljaju jasne i potpune informacije o obradi podataka koja se provodi putem sustava eCall. Informacije se navode u vlasničkom priručniku odvojeno za sustav eCall ugrađen u vozilo koji se temelji na službi 112 i za sve sustave eCall koji podržavaju usluge treće strane prije upotrebe tog sustava. Te informacije sadržavaju:

- upućivanje na pravnu osnovu za obradu
- činjenicu da se sustav eCall ugrađen u vozilo koji se temelji na službi 112 automatski aktivira
- načine obrade podataka koju provodi sustav eCall ugrađen u vozilo koji se temelji na službi 112
- posebnu svrhu obrade u okviru poziva sustava eCall, koja je ograničena na izvanredne situacije iz članka 5. stavka 2. prvog podstavka Uredbe (EU) 2015/758
- vrste prikupljenih i obrađenih podataka te primatelje tih podataka
- rok za zadržavanje podataka u sustavu eCall ugrađenom u vozilo koji se temelji na službi 112
- činjenicu da ne postoji stalno praćenje vozila
- načine ostvarivanja prava ispitanika te službu za kontakt odgovornu za obradu zahtjeva za pristup
- sve potrebne dodatne informacije u pogledu sljedivosti, praćenja i obrade osobnih podataka u vezi s pružanjem usluge eCall s trećom stranom kao pružateljem usluga (TPS eCall) i/ili drugih usluga s dodanom vrijednosti, koje podliježu izričitom pristanku vlasnika i u skladu su s Općom uredbom o zaštiti podataka. Posebno se vodi računa o tome da mogu postojati razlike između obrade podataka koja se provodi putem sustava eCall ugrađenog u vozilo koji se temelji na službi 112 i putem sustava TPS eCall ugrađenih u vozilo ili drugih usluga s dodanom vrijednosti.

139. Nadalje, davatelj usluga isto tako treba ispitanicima dostaviti informacije na transparentan i razumljiv način u skladu s člankom 13. Opće uredbe o zaštiti podataka. Posebno ih se mora obavijestiti o svrhama obrade za koju su osobni podaci namijenjeni i o tome da se obrada osobnih podataka temelji na pravnoj obvezi kojoj podliježe voditelj obrade.

140. Nadalje, uzimajući u obzir prirodu obrade, informacije o primateljima ili kategorijama primatelja osobnih podataka trebale bi biti jasne, a ispitanike bi trebalo obavijestiti da podaci nisu dostupni izvan sustava eCall ugrađenog u vozilo koji se temelji na službi 112 nikakvim subjektima prije aktiviranja poziva sustava eCall.

141. Kad je riječ o pravima ispitanika, treba napomenuti da se ne primjenjuju pravo na prigovor i pravo na prenosivost jer se obrada temelji na pravnoj obvezi.

3.2.5. Primatelj:

142. Podaci nisu dostupni izvan sustava ugrađenog u vozilo koji se temelji na službi 112 nikakvim subjektima prije aktiviranja poziva sustava eCall.

143. Kad se aktivira poziv sustava eCall (kad ga ručno aktiviraju putnici u vozilu ili se automatski aktivira čim ugrađeni senzor otkrije težak sudar), sustav eCall uspostavlja govornu vezu s odgovarajućim PSAP-om i MSD se šalje operateru PSAP-a.

144. Nadalje, podaci koji se prenose preko sustava eCall ugrađenog u vozilo koji se temelji na službi 112 te koje obrađuju PSAP-ovi mogu se proslijediti hitnoj službi i partnerima u pružanju usluga iz Odluke br. 585/2014/EU samo u slučaju incidenata povezanih s pozivima sustava eCall i pod uvjetima koji su utvrđeni u toj odluci, a upotrebljavaju se isključivo za ostvarivanje ciljeva te odluke. Podaci koje obrađuju PSAP-ovi putem sustava eCall ugrađenog u vozilo koji se temelji na službi 112 ne prosljeđuju se nijednoj trećoj strani bez izričitog prethodnog pristanka ispitanika.

3.2.6. Sigurnost

145. Uredbom (EU) 2015/758 utvrđeni su zahtjevi za ugrađivanje tehnologija za veću zaštitu privatnosti u sustav eCall kako bi korisnicima sustava pružile odgovarajuću razinu zaštite privatnosti te potrebna jamstva s ciljem sprečavanja nadziranja i zloupotrebe. Proizvođači bi usto trebali osigurati da su sustav eCall ugrađen u vozilo koji se temelje na službi 112 i svaki dodatni sustav koji pruža usluge eCall s trećom stranom kao pružateljem usluga ili uslugu s dodanom vrijednosti osmišljeni tako da nije moguća nikakva razmjena osobnih podataka između njih.

146. Kad je riječ o PSAP-ovima, države članice trebale bi osigurati da se osobni podaci zaštite od zloupotrebe, uključujući nezakoniti pristup, izmjenu ili gubitak, te da se protokoli o pohranjivanju, razdoblju zadržavanja, obradi i zaštiti osobnih podataka utvrde na odgovarajućoj razini i da ih se poštuje.

3.3. Studije o nesrećama

147. Ispitanici mogu dobrovoljno sudjelovati u studijama o nesrećama koje su posebno usmjerene na bolje razumijevanje uzroka prometnih nesreća i koje se provode u opće znanstvene svrhe.

3.3.1. Pravna osnova

148. Ako se podaci prikupljaju putem javne elektroničke komunikacijske usluge, voditelj obrade podataka morat će dobiti pristanak ispitanika za pristup informacijama koje su već pohranjene u vozilu kako je predviđeno člankom 5. stavkom 3. Direktive o e-privatnosti. Nijedno izuzeće predviđeno tim odredbama ne može se primijeniti u tom kontekstu: obrada se ne odvija isključivo u svrhu prijenosa komunikacije putem elektroničke komunikacijske mreže niti se odnosi na neku uslugu informacijskog društva koju je pretplatnik ili korisnik izričito zatražio.

149. Uzimajući u obzir raznolikost i količinu osobnih podataka potrebnih za studije o nesrećama, Odbor preporučuje da se obrada osobnih podataka temelji na prethodnoj privoli ispitanika u skladu s člankom 6. Opće uredbe o zaštiti podataka. Takva prethodna privola, kojom ispitanik pristaje na dobrovoljno sudjelovanje u studiji i obradu njegovih osobnih podataka u tu svrhu, mora se dati na posebnom obrascu. Privola je dobrovoljno, posebno i informirano izražavanje želja osobe čiji se podaci obrađuju (npr. označivanjem kućice koja nije prethodno označena ili konfiguracijom ugrađenog računala kojom se aktivira funkcija u vozilu). Takva se privola zbog određenih razloga daje odvojeno i ne može se dodati ugovoru o kupnji ili zakupu novog automobila, a povlačenje te privole mora biti jednako jednostavno kao njezino davanje. Povlačenje privole dovodi do zaustavljanja obrade. Tad se podaci brišu iz aktivne baze podataka ili se anonimiziraju.

150. Pristanak u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti i privola koja čini pravnu osnovu za obradu podataka mogu se prikupljati u isto vrijeme (primjerice označivanjem kućice kojim se jasno ukazuje na što ispitanik pristaje).

151. Treba napomenuti da se, ovisno o uvjetima obrade (priroda voditelja obrade podataka itd.), može zakonito odabrati druga pravna osnova sve dok se njome ne smanjuje dodatna zaštita predviđena člankom 5. stavkom 3. Direktive o e-privatnosti (vidjeti stavak 15.). Ako se obrada temelji na drugoj pravnoj osnovi, kao što je izvršavanje zadaće od javnog interesa (članak 6. stavak 1. točka (e) Opće uredbe o zaštiti podataka), Odbor preporučuje da ispitanici sudjeluju u studiji na dobrovoljnoj osnovi.

3.3.2. Prikupljeni podaci

152. Voditelj obrade podataka prikuplja samo osobne podatke koji su neophodni za obradu.

153. Dvije su vrste podataka koje treba uzeti u obzir:

- **podaci o sudionicima i vozilima**
- **tehnički podaci iz vozila** (trenutačna brzina itd.).

154. Znanstvena istraživanja o nesrećama opravdavaju prikupljanje podataka o trenutačnoj brzini, među ostalim i prikupljanje koje provode pravne osobe koje ne pružaju javne usluge u užem smislu.

155. Kao što je prethodno navedeno, Odbor smatra da podaci o trenutačnoj brzini prikupljeni u kontekstu studije o nesrećama nisu povezani s kaznenim djelima s obzirom na primatelja (tj. ne prikupljaju se u svrhu istrage ili progona kaznenih djela), pa je njihovo prikupljanje koje provode pravne osobe koje ne pružaju javne usluge u užem smislu opravdano.

3.3.3. Razdoblje zadržavanja

156. Važno je razlikovati dvije vrste podataka. Prvo, podaci o sudionicima i vozilima mogu se zadržati tijekom trajanja studije. Drugo, tehnički podaci iz vozila u tu se svrhu zadržavaju što kraće. U tom se smislu razdoblje od pet godina nakon završetka studije čini razumnim. Na kraju tog razdoblja podaci se brišu ili anonimiziraju.

3.3.4. Informiranje i prava ispitanika

157. Prije obrade osobnih podataka ispitaniku treba dostaviti informacije na transparentan i razumljiv način u skladu s člankom 13. Opće uredbe o zaštiti podataka. Točnije, ispitanike bi trebalo konkretno obavijestiti o prikupljanju ako se prikupljaju podaci o trenutačnoj brzini. Budući da se obrada podataka temelji na privoli, ispitanik se mora konkretno obavijestiti o pravu na povlačenje pristanka u bilo kojem trenutku, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena. Nadalje, budući da se u tom kontekstu podaci prikupljaju od ispitanika (na određenim obrascima ili njegovom aktivnošću) i obrađuju u skladu s člankom 6. stavkom 1. točkom (a) Opće uredbe o zaštiti podataka (privola), ispitanik ima pravo iskoristiti svoje pravo na prenosivost podataka. Kao što je naglašeno u smjernicama o pravu na prenosivost podataka, Odbor posebno preporučuje „da voditelji obrade jasno objasne razliku između vrsta podataka koje ispitanik može primiti na temelju prava na pristup ispitanika i prava na prenosivost podataka”. Stoga bi voditelj obrade podataka ispitanicima trebao osigurati jednostavan način da svoju privolu povuku dobrovoljno i u bilo kojem trenutku. Usto bi trebao razviti alate za odgovaranje na zahtjeve za prenosivost podataka.

158. Te se informacije mogu dati nakon potpisivanja obrasca u kojem se pristaje sudjelovati u studiji o nesrećama.

3.3.5. Primatelj

159. Načelno samo voditelj i izvršitelj obrade podataka imaju pristup podacima.

3.3.6. Sigurnost

160. Kako je prethodno navedeno, uspostavljene sigurnosne mjere prilagođavaju se razini osjetljivosti podataka. Primjerice, ako se podaci o trenutačnoj brzini (ili bilo koji drugi podaci

o kaznenim osudama i kaznenim djelima) prikupljaju u okviru studije o nesrećama, Odbor čvrsto preporučuje uspostavljanje strogih sigurnosnih mjera, kao što su:

- provedba mjera pseudonimizacije (npr. raspršivanje podataka tajnim ključem, primjerice prezimena/imena ispitanika i serijskog broja)
- pohrana podataka o trenutačnoj brzini i lokaciji u odvojenim bazama podataka (npr. upotrebom najsuvremenijeg mehanizma šifriranja s različitim ključevima i mehanizmima za odobravanje)
- i/ili brisanje podataka o lokaciji čim se kvalificira referentni događaj ili slijed događaja (npr. vrsta ceste, dan/noć) i pohrana podataka iz kojih se može izravno utvrditi identitet u posebnu bazu podataka kojoj može pristupiti samo mali broj ljudi.

3.4. Rješavanje problema krađe automobila

161. U slučaju krađe ispitanik može pokušati pronaći svoje vozilo upotrebom podataka o lokaciji. Upotreba podataka o lokaciji ograničena je na prijeke potrebe istrage i na procjenu slučaja koju provode nadležna pravosudna tijela.

3.4.1. Pravna osnova

162. Kad se podaci prikupljaju putem javno dostupne elektroničke komunikacijske usluge, primjenjuje se članak 5. stavak 3. Direktive o e-privatnosti.

163. Budući da je to usluga informacijskog društva, člankom 5. stavkom 3. Direktive o e-privatnosti ne zahtijeva se pristanak za pristup informacijama koje su već pohranjene u vozilu u slučaju kad pretplatnik ili korisnik izričito zatraži takvu uslugu.

164. Kad je riječ o obradi osobnih podataka, pravna osnova za obradu podataka o lokaciji bit će pristanak vlasnika vozila ili, ako je primjenjivo, izvršenje ugovora (samo za podatke nužne za izvršenje ugovora kojem je ispitanik stranka).

165. Pristanak je dobrovoljno, posebno i informirano izražavanje želja osobe čiji se podaci obrađuju (npr. označivanjem kućice koja nije prethodno označena ili konfiguracijom ugrađenog računala kojom se aktivira funkcija u vozilu). Sloboda davanja pristanka uključuje mogućnost povlačenja pristanka u bilo kojem trenutku, o čemu bi ispitanika trebalo izričito obavijestiti. Povlačenje pristanka dovodi do zaustavljanja obrade. Tad se podaci brišu iz aktivne baze podataka, anonimiziraju ili arhiviraju.

3.4.2. Prikupljeni podaci

166. Podaci o lokaciji mogu se prenositi isključivo nakon prijave krađe i ne smiju se neprekidno prikupljati ostatak vremena.

3.4.3. Razdoblje zadržavanja

167. Podaci o lokaciji mogu se zadržavati samo u razdoblju tijekom kojeg nadležna pravosudna tijela procjenjuju slučaj ili do okončanja postupka uklanjanja sumnje koji ne završava potvrdom krađe vozila.

3.4.4. Informiranje ispitanika

168. Prije obrade osobnih podataka ispitanika bi o tome trebalo obavijestiti na transparentan i razumljiv način u skladu s člankom 13. Opće uredbe o zaštiti podataka. Konkretnije, Odbor preporučuje da voditelj obrade podataka naglasi da se vozilo ne prati neprestano i da se podaci o lokaciji mogu prikupljati i prenositi samo nakon prijave krađe. Nadalje, voditelj obrade ispitanika mora obavijestiti o tome da pristup podacima imaju samo odobreni službenici platforme za nadzor na daljinu i pravno odobrena tijela.

169. Kad je riječ o pravima ispitanika, ispitanika bi, kad se obrada podataka temelji na pristanku, trebalo konkretno obavijestiti o pravu na povlačenje pristanka u bilo kojem trenutku, a da

to ne utječe na zakonitost obrade koja se temeljila na pristanku prije nego što je on povučen. Budući da u se u tom kontekstu podaci prikupljaju od ispitanika (na određenim obrascima ili njegovom aktivnošću) i obrađuju u skladu s člankom 6. stavkom 1. točkom (a) (privola) ili člankom 6. stavkom 1. točkom (b) (izvršavanje ugovora) Opće uredbe o zaštiti podataka, ispitanik ima pravo ostvariti svoje pravo na prenosivost podataka. Kao što je naglašeno u smjernicama o pravu na prenosivost podataka, Odbor posebno preporučuje „da voditelji obrade jasno objasne razliku između vrsta podataka koje ispitanik može primiti na temelju prava na pristup ispitanika i prava na prenosivost podataka”.

170. Stoga bi voditelj obrade podataka trebao osigurati ispitanicima jednostavan način da svoj pristanak (samo ako čini pravnu osnovu) povuku slobodno i u bilo kojem trenutku. Usto bi trebao razviti alate za odgovaranje na zahtjeve za prenosivost podataka.

171. Informacije se mogu dostaviti nakon potpisivanja ugovora.

3.4.5. Primatelji

172. U slučaju prijave krađe podaci o lokaciji mogu se prenositi i. odobrenim službenicima platforme za nadzor na daljinu i ii. pravno odobrenim tijelima.

3.4.6. Sigurnost

173. Primjenjuju se opće preporuke. Vidjeti odjeljak 2.7.