

# Smernice



**Smernice 01/2020 o obdelavi osebnih podatkov v okviru  
povezanih vozil in aplikacij, povezanih z mobilnostjo**

**Različica 2.0**

**Sprejete 9. marca 2021**

## Zgodovina različic

Različica 2.0	9. marec 2021	Sprejetje smernic po javnem posvetovanju
Različica 1.0	28. januar 2020	Sprejetje smernic za javno posvetovanje

## Vsebina

1	UVOD .....	4
1.1	Povezana dela.....	5
1.2	Pravo, ki se uporablja .....	6
1.3	Področje uporabe .....	8
1.4	Opredelitev pojmov.....	11
1.5	Tveganja za zasebnost in varstvo podatkov .....	14
2	SPLOŠNA PRIPOROČILA .....	16
2.1	Kategorije podatkov .....	16
2.2	Nameni .....	18
2.3	Ustreznost in najmanjši obseg podatkov .....	19
2.4	Vgrajeno in privzeto varstvo podatkov .....	19
2.5	Informacije .....	22
2.6	Pravice posameznika, na katerega se nanašajo osebni podatki .....	25
2.7	Varnost .....	25
2.8	Posredovanje osebnih podatkov tretjim osebam .....	26
2.9	Prenos osebnih podatkov zunaj EU/EGP.....	27
2.10	Uporaba tehnologij Wi-Fi v vozilu .....	28
3	ŠTUDIJE PRIMEROV .....	28
3.1	Zagotavljanje storitve s strani tretje osebe.....	28
3.2	eCall.....	32
3.3	Študije na področju preučevanja in analiziranja vzrokov in posledic nesreč.....	35
3.4	Obnavljanje kraje avtomobila .....	37

## Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018<sup>1</sup>,

ob upoštevanju členov 12 in 22 svojega poslovnika –

### SPREJEL NASLEDNJE SMERNICE:

## 1 UVOD

1. Avtomobil, simbol gospodarstva 20. stoletja, je eden od izdelkov široke porabe, ki je vplival na družbo kot celoto. Avtomobili, ki se na splošno povezujejo s pojmom svobode, pogosto veljajo za več kot samo prevozno sredstvo. Predstavljajo namreč zasebni prostor, v katerem lahko ljudje uživajo obliko avtonomije odločanja, ne da bi se srečevali z zunanjimi poseganji. Danes, ko povezana vozila prehajajo v splošno uporabo, tak pogled ni več odraz realnosti. Povezljivost v vozilu se hitro širi z luksuznih modelov in vrhunskih znamk na številne modele srednjega cenovnega razreda, vozila pa postajajo obsežna podatkovna vozlišča. Povezana niso samo vozila, temveč čedalje bolj povezani postajajo tudi vozniki in potniki. Dejansko številni modeli, ki so bili v zadnjih nekaj letih dani na trg, vključujejo senzorje in povezano opremo v vozilu, ki lahko med drugim zbira in zapisuje podatke o zmogljivosti motorja, voznih navadah, obiskanih lokacijah in potencialno celo o voznikovem premikanju oči ter njegovem srčnem utripu ali biometrične podatke za edinstveno identifikacijo posameznika<sup>2</sup>.
2. Taka obdelava podatkov poteka v zapletenem ekosistemu, ki ni omejen na tradicionalne akterje v avtomobilski industriji, ampak ga oblikuje tudi pojav novih akterjev v digitalnem gospodarstvu. Ti novi akterji lahko ponujajo informacijsko-razvedrilne storitve, kot so spletna glasba ter informacije o stanju na cestah in prometu, ali zagotavljajo sisteme in storitve za pomoč pri vožnji, kot so programska oprema za avtopilota, najnovejše informacije o stanju vozila, zavarovanje na podlagi uporabe ali dinamično kartiranje. Ker so vozila povezana prek elektronskih komunikacijskih omrežij, imajo poleg tega tudi upravljavci cestne infrastrukture in telekomunikacijski operaterji, vključeni v ta proces, pomembno vlogo pri morebitnih dejanjih obdelave osebnih podatkov voznikov in potnikov.
3. Povezana vozila tudi ustvarjajo čedalje večje količine podatkov, ki jih je večinoma mogoče šteti za osebne podatke, saj se nanašajo na voznike ali potnike. Čeprav podatki, ki jih zbira

---

<sup>1</sup> Sklicevanja na „države članice“ v tem dokumentu je treba razumeti kot sklicevanja na „države članice EGP“.

<sup>2</sup> Infografika „Podatki in povezani avtomobil“, ki jo je pripravil Future of Privacy Forum; [https://fpf.org/wp-content/uploads/2017/06/2017\\_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf](https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf).

povezani avtomobil, niso neposredno povezani z imenom, ampak s tehničnimi vidiki in lastnostmi vozila, zadevajo voznika ali potnike v avtomobilu. Za ponazoritev, podatki o slogu vožnje ali prevoženi razdalji, podatki o obrabi delov vozila, podatki o lokaciji ali podatki, ki jih zberejo kamere, se lahko nanašajo na voznikovo vedenje, pa tudi na informacije o drugih ljudeh, ki so morda v vozilu, ali mimoidočih posameznikih, na katere se nanašajo osebni podatki. Take tehnične podatke proizvede posameznik, ti pa omogočajo njegovo neposredno ali posredno identifikacijo s strani upravljavca podatkov ali druge osebe. Vozilo je mogoče šteti za terminal, ki ga lahko uporabljajo različni uporabniki. Zato tako kot pri osebnem računalniku ta možnost obstoja več uporabnikov ne vpliva na osebno naravo podatkov.

4. Leta 2016 je združenje Fédération Internationale de l'Automobile (FIA) po Evropi izvedlo kampanjo „Moj avtomobil, moji podatki“, da bi dobilo vpogled v mnenje Evropejcev in Evropejk o povezanih avtomobilih<sup>3</sup>. Čeprav je kampanja pokazala veliko zanimanje voznikov za povezljivost, pa je izpostavila tudi pazljivost, ki je potrebna pri uporabi podatkov, ki jih proizvedejo vozila, in pomen upoštevanja zakonodaje o varstvu osebnih podatkov. Izziv za vsakega deležnika je torej, da že od faze zasnove izdelka upošteva vidik „varstva osebnih podatkov“ ter zagotovi, da uporabniki avtomobilov uživajo preglednost in nadzor v zvezi s svojimi podatki v skladu z uvodno izjavo 78 Splošne uredbe o varstvu podatkov. Tak pristop prispeva h krepitvi zaupanja uporabnikov in torej k dolgoročnemu razvoju zadevnih tehnologij.

## 1.1 Povezana dela

5. Povezana vozila so v zadnjem desetletju, še zlasti pa v zadnjih nekaj letih, postala pomembna tema za regulativne organe. Na nacionalni in mednarodni ravni so bila zato objavljena različna dela, ki se nanašajo na varnost in zasebnost povezanih vozil. Namen teh predpisov in pobud je dopolniti veljavne okvire varstva podatkov in zasebnosti s sektorskimi pravili ali zagotoviti smernice za strokovnjake.

### 1.1.1 Pobude na evropski ravni in mednarodne pobude

6. Od 31. marca 2018 je pri vseh novih tipih vozil kategorij M1 in N1 (osebni avtomobili in lahka vozila) obvezen sistem eCall, vgrajen v vozilo, kot storitev številke 112<sup>4,5</sup>. Delovna skupina iz člena 29 je leta 2006 že sprejela delovni dokument o posledicah pobude eCall za varstvo podatkov in zasebnost<sup>6</sup>. Poleg tega je, kot je bilo predhodno obravnavano, Delovna skupina iz člena 29. oktobra 2017 sprejela tudi mnenje o obdelavi osebnih podatkov v okviru sodelovalnih inteligentnih prometnih sistemov (C-ITS).
7. Agencija Evropske unije za varnost omrežij in informacij (ENISA) je januarja 2017 objavila študijo, osredinjeno na kibernetsko varnost in odpornost pametnih avtomobilov, v kateri je navedla občutljiva sredstva ter ustrezne grožnje, tveganja, blažilne dejavnike in mogoče

---

<sup>3</sup> Kampanja „Moj avtomobil, moji podatki“; <http://www.mycarmydata.eu/>.

<sup>4</sup> Interoperabilni vseevropski eCall; [https://ec.europa.eu/transport/themes/its/road/action\\_plan/ecall\\_en](https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en).

<sup>5</sup> Sklep št. 585/2014/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o uvedbi medobratovalne vseevropske storitve eCall (Besedilo velja za EGP); <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32014D0585>.

<sup>6</sup> Delovni dokument o možnih posledicah sistema eCall za varstvo podatkov in zasebnost; [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125\\_sl.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_sl.pdf).

varnostne ukrepe za izvedbo<sup>7</sup>. Septembra 2017 je Mednarodna konferenca pooblaščenec za varstvo podatkov in zasebnost (ICDPPC) sprejela resolucijo o povezanih vozilih<sup>8</sup>. Nazadnje, aprila 2018 je Mednarodna skupina za varstvo osebnih podatkov v telekomunikacijah (IWGDPT) prav tako sprejela delovni dokument o povezanih vozilih<sup>9</sup>.

### 1.1.2 Nacionalne pobude članov Evropskega odbora za varstvo podatkov

8. Januarja 2016 sta konferenca nemških zveznih in deželnih organov za varstvo podatkov ter nemško združenje avtomobilske industrije (VDA) objavila skupno izjavo o načelih varstva podatkov v povezanih in nepovezanih vozilih<sup>10</sup>. Avgusta 2017 je center Združenega kraljestva za povezana in avtonomna vozila (Centre for Connected and Autonomous Vehicles – CCAV) izdal vodnik, v katerem so navedena načela kibernetike varnosti za povezana in avtomatizirana vozila, da bi se povečala ozaveščenost o tej zadevi v avtomobilskem sektorju<sup>11</sup>. Oktobra 2017 je francoski organ za varstvo podatkov, tj. Commission Nationale de l'Informatique et des Libertés (CNIL), izdal sveženj za skladnost za povezane avtomobile, da bi deležnikom pomagal pri tem, kako vključiti vgrajeno in privzeto varstvo podatkov, s čimer bi bil posameznikom, na katere se nanašajo osebni podatki, omogočen učinkovit nadzor nad njihovimi podatki<sup>12</sup>.

## 1.2 Pravo, ki se uporablja

9. Upoštevni pravni okvir EU je Splošna uredba o varstvu podatkov. Uporablja se vedno, kadar obdelava podatkov v okviru povezanih vozil vključuje obdelavo osebnih podatkov posameznikov.
10. Poleg Splošne uredbe o varstvu podatkov Direktiva 2002/58/ES, kot je bila revidirana z Direktivo 2009/136/ES (v nadaljevanju: direktiva o e-zasebnosti), **določa poseben standard za vse akterje, ki želijo shranjevati podatke ali dostopati do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika v Evropskem gospodarskem prostoru (EGP)**.
11. Večina določb direktive o e-zasebnosti (člena 6, 9 itd.) se uporablja samo za ponudnike javno dostopnih elektronskih komunikacijskih storitev in ponudnike javnih komunikacijskih omrežij, člen 5(3) direktive o e-zasebnosti pa je splošna določba. Ne uporablja se samo za elektronske komunikacijske storitve, ampak tudi za vsak zasebni ali javni subjekt, ki podatke shrani v terminalski opremi ali jih prebere iz nje, ne glede na naravo podatkov, ki so shranjeni ali do katerih se dostopa.

---

<sup>7</sup> Kibernetika varnost in odpornost pametnih avtomobilov; <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.

<sup>8</sup> Resolucija o varstvu podatkov v avtomatiziranih in povezanih vozilih; [https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles\\_en\\_1.pdf](https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf).

<sup>9</sup> Delovni dokument o povezanih vozilih; <https://www.datenschutz-berlin.de/infotehk-und-service/veroeffentlichungen/working-paper/>.

<sup>10</sup> Vidiki varstva podatkov pri uporabi povezanih in nepovezanih vozil; [https://www.lda.bayern.de/media/dsk\\_joint\\_statement\\_vda.pdf](https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf).

<sup>11</sup> Načela kibernetike varnosti za povezana in avtomatizirana vozila; <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>.

<sup>12</sup> Sveženj za skladnost za odgovorno uporabo podatkov v povezanih avtomobilih; <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>.

12. Pojem „terminalska oprema“ je opredeljen v Direktivi 2008/63/ES<sup>13</sup>. V skladu z njenim členom 1(a) terminalska oprema pomeni „vso opremo, ki je neposredno ali posredno priključena na mrežni vmesnik javnega telekomunikacijskega omrežja za pošiljanje, obdelovanje ali sprejemanje informacij; v obeh primerih (neposredna ali posredna) se lahko priključitev izvede z žico, optičnim kablom ali elektromagnetno; priključitev je posredna, če je oprema nameščena med terminalom in javnim mrežnim vmesnikom; (b) pomeni tudi opremo satelitskih zemeljskih postaj“.
13. Posledično je treba, če so zgornja merila izpolnjena, povezano vozilo in napravo, priključeno nanj, šteti za „terminalsko opremo“ (tako kot računalnik, pametni telefon ali pametno televizijo) in se, kjer je to ustrezno, uporabljajo določbe člena 5(3) direktive o e-zasebnosti.
14. Kot je Evropski odbor za varstvo podatkov poudaril v svojem mnenju št. 5/2019 o medsebojnem vplivu direktive o e-zasebnosti in Splošne uredbe o varstvu podatkov<sup>14</sup>, člen 5(3) direktive o e-zasebnosti določa, da je praviloma in ob upoštevanju izjem od tega pravila, navedenih v odstavku 17 spodaj, za shranjevanje podatkov ali pridobivanje dostopa do podatkov, ki so že shranjeni v terminalski opremi naročnika ali uporabnika, potrebna predhodna privolitev. Če so podatki, shranjeni v napravi končnega uporabnika, osebni podatki, ima člen 5(3) direktive o e-zasebnosti prednost pred členom 6 Splošne uredbe o varstvu podatkov, glede dejavnosti shranjevanja teh podatkov ali pridobivanja dostopa do njih<sup>15</sup>. Vsa dejanja obdelave osebnih podatkov po zgoraj navedenih dejanjih obdelave, vključno z obdelavo osebnih podatkov, pridobljenih z dostopom do podatkov v terminalski opremi, morajo temeljiti na pravni podlagi iz člena 6 Splošne uredbe o varstvu podatkov, da bi bila zakonita<sup>16</sup>.
15. Ker bo moral upravljavec, ko bo želel dobiti privolitev za shranjevanje podatkov ali pridobivanje dostopa do podatkov v skladu s členom 5(3) direktive o e-zasebnosti, posameznika, na katerega se nanašajo osebni podatki, obvestiti o vseh namenih obdelave – vključno z vsako obdelavo po zgoraj navedenih dejanjih (kar pomeni „nadaljnjo obdelavo“) –, bo privolitev na podlagi člena 6 Splošne uredbe o varstvu podatkov običajno najustreznejša pravna podlaga za obdelavo osebnih podatkov po takih dejanjih (če je namen nadaljnje obdelave zajet s privolitvijo posameznika, na katerega se nanašajo osebni podatki, glej odstavka 53 in 54 spodaj). Privolitev bo torej verjetno pravna podlaga tako za shranjevanje podatkov in pridobivanje dostopa do že shranjenih podatkov kot tudi za nadaljnjo obdelavo osebnih podatkov<sup>17</sup>. Pri oceni skladnosti s členom 6 Splošne uredbe o

---

<sup>13</sup> Direktiva Komisije 2008/63/ES z dne 20. junija 2008 o konkurenci na trgih za telekomunikacijsko terminalsko opremo (Kodificirana različica) (besedilo velja za EGP); <https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX%3A32008L0063>.

<sup>14</sup> Evropski odbor za varstvo podatkov, Mnenje št. 5/2019 o medsebojnem vplivu Direktive o zasebnosti in elektronskih komunikacijah in Splošne uredbe o varstvu podatkov, zlasti v zvezi s pristojnostmi, nalogami in pooblastili organov za varstvo podatkov, sprejeto 12. marca 2019 (v nadaljevanju: Mnenje št. 5/2019), odstavek 40.

<sup>15</sup> Prav tam, odstavek 40.

<sup>16</sup> Prav tam, odstavek 41.

<sup>17</sup> Privolitev, ki se zahteva s členom 5(3) direktive o e-zasebnosti, in privolitev, potrebna kot pravna podlaga za obdelavo podatkov (člen 6 Splošne uredbe o varstvu podatkov) za isti konkretni namen, se lahko pridobita sočasno (na primer z označitvijo okenca, ob katerem je jasno navedeno, v kaj bo privolil posameznik, na katerega se nanašajo osebni podatki).

varstvu podatkov bi bilo namreč treba upoštevati, da obdelava kot celota vključuje posebne dejavnosti, v zvezi s katerimi si je zakonodajalec EU prizadeval zagotoviti dodatno varstvo<sup>18</sup>. Poleg tega morajo upravljavci pri določanju ustrezne zakonite podlage upoštevati vpliv na pravice posameznikov, na katere se nanašajo osebni podatki, da bi se upoštevalo načelo pravičnosti<sup>19</sup>. Bistvo je, da se upravljavci ne morejo opreti na člen 6 Splošne uredbe o varstvu podatkov, da bi zmanjšali dodatno varstvo, določeno s členom 5(3) direktive o e-zasebnosti.

16. Evropski odbor za varstvo podatkov opozarja, da pojem privolitve v direktivi o e-zasebnosti ostaja pojem privolitve v Splošni uredbi o varstvu podatkov in mora izpolnjevati vse zahteve za privolitev, kot so določene s členoma 4(11) in 7 Splošne uredbe o varstvu podatkov.
17. Čeprav je načelo privolitev, pa člen 5(3) direktive o e-zasebnosti omogoča, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, ki so že shranjeni v terminalski opremi, izvzeto iz zahteve po informirani privolitvi, če izpolnjuje eno od naslednjih meril:
  - )] **izjema 1:** izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja;
  - )] **izjema 2:** če je nujno potrebno, da ponudnik storitve informacijske družbe zagotovi storitev, ki jo naročnik ali uporabnik izrecno zahteva.
18. V takih primerih obdelava osebnih podatkov, vključno z obdelavo osebnih podatkov, pridobljenih z dostopom do podatkov v terminalski opremi, temelji na eni od pravnih podlag, kot so določene v členu 6 Splošne uredbe o varstvu podatkov. Privolitev na primer ni potrebna, kadar je obdelava podatkov potrebna za zagotovitev navigacijskih storitev GPS, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, kadar je take storitve mogoče opredeliti kot storitve informacijske družbe.

### 1.3 Področje uporabe

19. Evropski odbor za varstvo podatkov poudarja, da so te smernice namenjene olajšanju skladnosti obdelave osebnih podatkov, ki jo izvajajo številni različni deležniki, ki delujejo v tem okolju. Vendar njihov namen ni zajeti vse mogoče primere uporabe v tem okviru ali zagotoviti smernice za vsak mogoč konkreten položaj.
20. Ta dokument je osredinjen zlasti na obdelavo osebnih podatkov v zvezi z nepoklicno uporabo povezanih vozil s strani posameznikov, na katere se nanašajo osebni podatki, na primer voznikov, potnikov, lastnikov vozil, drugih udeležencev v prometu itd. Natančneje, obravnava osebne podatke: (i) obdelane v vozilu, (ii) izmenjane med vozilom in osebnimi napravami, priključenimi nanj (na primer uporabnikovim pametnim telefonom), ali (iii) zbrane lokalno v vozilu in izvožene zunanjim subjektom (na primer proizvajalcem vozil, upravljavcem infrastrukture, zavarovalnicam, avtomehanikom) za nadaljnjo obdelavo.

---

<sup>18</sup> Mnenje št. 5/2019, odstavek 41.

<sup>19</sup> Evropski odbor za varstvo podatkov, Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, različica 2.0, 8. oktober 2019, odstavek 1.



21. Povezano vozilo je treba v tem dokumentu razumeti kot širok pojem. Opredeliti ga je mogoče kot vozilo, opremljeno s številnimi elektronskimi krmilnimi enotami, ki so med seboj povezane prek omrežja v vozilu, in napravami za povezljivost, ki mu omogočajo izmenjavo podatkov z drugimi napravami znotraj in zunaj vozila. Tako se podatki lahko izmenjujejo med vozilom in osebnimi napravami, povezanimi z njim, kar na primer omogoča prikazovanje mobilnih aplikacij na enoti armaturne plošče avtomobila za informacije in razvedrilo. Prav tako je del področja uporabe tega dokumenta tudi razvoj samostojnih mobilnih aplikacij, kar pomeni neodvisnih od vozila (ki se na primer opirajo samo na uporabo pametnega telefona), za pomoč voznikom, saj pripomorejo k zmogljivostim vozila za povezljivost, čeprav se morda dejansko ne opirajo na prenos podatkov s samim vozilom. Aplikacije za povezana vozila so številne in raznolike ter lahko vključujejo<sup>20</sup>:
22. *Upravljanje mobilnosti*: funkcije, ki voznikom omogočajo, da na cilj prispejo hitro in stroškovno učinkovito, tako da zagotavljajo pravočasne informacije o navigaciji GPS, morebiti nevarnih okoljskih razmerah (na primer poledenele ceste), prometnih zastojev ali delu na cesti, pomoči v zvezi s parkirnim mestom ali garažo, optimizirani porabi goriva ali cestninah.
23. *Upravljanje vozila*: funkcije, ki naj bi voznikom pomagale znižati stroške delovanja in poenostaviti uporabo, kot so obvestilo o stanju vozila in opomniki za servisni pregled vozila, prenos podatkov o uporabi (na primer za storitve popravila vozila), prilagojena zavarovanja „plačaj, kolikor voziš/kako voziš“, operacije na daljavo (na primer sistem ogrevanja) ali konfiguracije profila (na primer nastavitve sedeža).
24. *Varnost v cestnem prometu*: funkcije, ki voznika opozarjajo na zunanje nevarnosti in notranje odzive, kot so zaščita pred trkom, opozorila na nevarnost, opozorila pred zapustitvijo voznega pasu, zaznavanje zaspanosti voznika, klic v sili (eCall) ali „črne skrinjice“ za preiskovanje nesreč (zapisovalnik podatkov o dogodku).
25. *Razvedrilo*: funkcije, ki vozniku in potnikom zagotavljajo informacije in razvedrilo, kot so vmesniki za pametne telefone (prostoročni telefonski klici, glasovno ustvarjena besedilna sporočila), dostopne točke WLAN, glasba, videoposnetki, družbeni mediji, mobilna pisarna ali storitve „pametnega doma“.
26. *Pomoč vozniku*: funkcije, ki vključujejo popolnoma ali delno avtomatizirano vožnjo, kot je operativna pomoč ali avtopilot v gostem prometu, pri parkiranju ali na avtocestah.
27. *Dobro počutje*: funkcije, ki spremljajo voznikovo udobje, sposobnost in primernost za vožnjo, kot je zaznavanje utrujenosti ali medicinska pomoč.
28. Vozila so torej lahko izvorno povezana ali ne, osebni podatki pa se lahko zbirajo z več sredstvi, med katerimi so: (i) senzorji vozila, (ii) telematske skrinjice ali (iii) mobilne aplikacije (na primer dostop iz naprave, ki pripada vozniku). Da bi mobilne aplikacije spadale na področje uporabe tega dokumenta, morajo biti povezane z okoljem vožnje. Na njegovo področje uporabe na primer spadajo aplikacije za navigacijo GPS. Vendar pa

---

<sup>20</sup> Strategija PwC za leto 2014. „In the fast lane. The bright future of connected cars“ (Na hitrem pasu. Svetla prihodnost povezanih avtomobilov): [https://www.strategyand.pwc.com/media/file/Strategyand\\_In-the-Fast-Lane.pdf](https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf).

aplikacije, ki voznikom samo predlagajo zanimive kraje (restavracije, zgodovinski spomenik itd.), ne spadajo na področje uporabe teh smernic.

29. Veliko podatkov, ki jih ustvari povezano vozilo, se nanaša na posameznika, ki je določen ali določljiv, in torej pomenijo osebne podatke. Podatki na primer vključujejo neposredno določljive podatke (na primer popolno identiteto voznika) in tudi posredno določljive podatke, kot so podrobnosti o opravljenih poteh, podatki o uporabi vozila (na primer podatki o slogu vožnje ali prepeljani razdalji) ali tehnični podatki o vozilu (na primer podatki o obrabi delov vozila), ki jih je mogoče z navzkrižnim povezovanjem z drugimi datotekami in zlasti identifikacijsko številko vozila (VIN) povezati s posameznikom. Osebni podatki v povezanih vozilih lahko vključujejo tudi metapodatke, kot je stanje vzdrževanja vozila. Povedano drugače, na področje uporabe tega dokumenta torej spadajo vsi podatki, ki jih je mogoče povezati s posameznikom.
30. Ekosistem povezanega vozila zajema širok spekter deležnikov. Ta ekosistem natančneje vključuje tradicionalne akterje iz avtomobilske industrije in prihajajoče akterje iz digitalne industrije. Zato so te smernice namenjene proizvajalcem vozil, proizvajalcem opreme in dobaviteljem v avtomobilski industriji, avtomehanicom, trgovcem z avtomobili, ponudnikom storitev za vozila, upravljavcem voznega parka, zavarovalnicam za motorna vozila, ponudnikom razvedrila, telekomunikacijskim operaterjem, upravljavcem cestne infrastrukture in javnim organom ter posameznikom, na katere se nanašajo osebni podatki. Evropski odbor za varstvo podatkov poudarja, da se bodo kategorije posameznikov, na katere se nanašajo osebni podatki, razlikovale od ene storitve do druge (na primer vozniki, lastniki, potniki itd.). To je neizčrpen seznam, saj ekosistem vključuje številne različne storitve, vključno s storitvami, za katere je potrebna neposredna avtentikacija ali identifikacija, in storitvami, za katere ta ni potrebna.
31. Določena obdelava podatkov, ki jo posamezniki opravijo v vozilu, spada v okvir „popolnoma osebne ali domače dejavnosti“, zato ne spada na področje uporabe Splošne uredbe o varstvu podatkov<sup>21</sup>. To se zlasti nanaša na uporabo osebnih podatkov v vozilih s strani samih posameznikov, na katere se nanašajo osebni podatki, ki so take podatke vnesli v armaturno ploščo vozila. Vendar Evropski odbor za varstvo podatkov opozarja, da se Splošna uredba o varstvu podatkov glede na njeno uvodno izjavo 18 „uporablja za upravljavce ali obdelovalce, ki zagotavljajo sredstva za obdelavo osebnih podatkov za take osebne ali domače dejavnosti“.

### 1.3.1 Zunaj področja uporabe tega dokumenta

32. Delodajalci, ki članom svojega osebja dajo na voljo službene avtomobile, bodo morda želeli spremljati dejanja svojih zaposlenih (na primer da bi zagotovili varnost zaposlenega, blaga ali vozil, razporedili sredstva, spremljali in obračunali storitev ali preverili delovni čas). Obdelava podatkov, ki jo v tem okviru izvajajo delodajalci, sproža posebne razmisleke za zaposlitveni okvir, ki bi lahko bili urejeni z delovno zakonodajo na nacionalni ravni, ki je ni mogoče podrobno predstaviti v teh smernicah<sup>22</sup>.
33. Čeprav lahko obdelava podatkov v okviru gospodarskih vozil, ki se uporabljajo za poklicne namene (kot je javni prevoz), skupnega prevoza in rešitve mobilnosti kot storitve odpira

<sup>21</sup> Glej Splošno uredbo o varstvu podatkov, člen 2(2)(c).

<sup>22</sup> Delovna skupina iz člena 29 je to obravnavala v svojem mnenju št. 2/2017 o obdelavi podatkov pri delu (WP249); [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610169](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

posebne razmisleke, ki ne spadajo na področje uporabe teh splošnih smernic, se bodo številna tu predstavljena načela in priporočila uporabljala tudi za te vrste obdelave.

34. Ker so povezana vozila radijsko omogočeni sistemi, so predmet pasivnega sledenja, kot je sledenje prek omrežij Wi-Fi ali Bluetooth. V tem smislu se ne razlikujejo od drugih povezanih naprav in spadajo na področje uporabe direktive o e-zasebnosti, ki se trenutno revidira. To torej izključuje tudi obsežno sledenje vozilom, opremljenim s povezavo Wi-Fi<sup>23</sup>, s strani goste mreže mimoidočih, ki uporabljajo običajne lokacijske storitve pametnih telefonov. Te rutinsko sporočajo vsa vidna omrežja Wi-Fi osrednjim strežnikom. Ker je mogoče vgrajeno povezavo Wi-Fi šteti za sekundarni identifikator vozila<sup>24</sup>, to pomeni tveganje za stalno zbiranje celovitih profilov gibanja vozila.
35. Čedalje več vozil je opremljenih z napravami za zajem slike (na primer sistemi kamer za parkiranje avtomobila ali kamerami na armaturni plošči). Ker se to nanaša na vprašanje snemanja javnih krajev, ki zahteva oceno ustreznega zakonodajnega okvira, specifičnega za vsako državo članico, ta obdelava podatkov ne spada na področje uporabe teh smernic.
36. Obdelava podatkov, ki omogoča sodelovalne inteligentne prometne sisteme (C-ITS), kot so opredeljeni v Direktivi 2010/40/EU<sup>25</sup>, je bila obravnavana v posebnem mnenju Delovne skupine iz člena 29<sup>26</sup>. Čeprav opredelitev pojma sistemov C-ITS v Direktivi ne vsebuje nobenih tehničnih specifikacij, se Delovna skupina iz člena 29 v svojem mnenju osredinja na komunikacije kratkega dosega, tj. ki ne vključujejo posredovanja omrežnega operaterja. Natančneje, zagotavlja analizo za posebne primere uporabe za začetno vzpostavitev in se je zavezala, da bo pozneje ocenila nova vprašanja, ki se bodo nedvomno pojavila, ko bo uvedena višja raven avtomatizacije. Ker so posledice varstva podatkov v okviru sistemov C-ITS zelo specifične (količine podatkov o lokaciji, kot jih še ni bilo, stalno oddajanje osebnih podatkov, izmenjava podatkov med vozili in drugimi napravami cestne infrastrukture itd.) in ker se o tem še vedno razpravlja na evropski ravni, obdelava osebnih podatkov v tem okviru ni zajeta v teh smernicah.
37. Nazadnje, namen tega dokumenta ni obravnavati vse mogoče težave in vprašanja, ki se pojavljajo glede povezanih vozil, zato ga ni mogoče šteti za izčrpnega.

#### 1.4 Opredelitev pojmov

38. **Obdelava** osebnih podatkov zajema vsako dejanje, ki vključuje osebne podatke, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje,

---

<sup>23</sup> Za podrobnosti glej: <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html>.

<sup>24</sup> Markus Ullmann, Tobias Franz in Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements (Identifikacija vozila na podlagi sekundarnega identifikatorja vozila – Analiza in meritve), v zborniku VEHICULAR 2017, Šesta mednarodna konferenca o napredku v prometnih sistemih, tehnologijah in aplikacijah, Nica, Francija, od 23. do 27. julija 2017, str. 32–37.

<sup>25</sup> Direktiva 2010/40/EU z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza; <https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32010L0040>.

<sup>26</sup> Delovna skupina iz člena 29 – Mnenje št. 03/2017 o obdelavi osebnih podatkov v okviru sodelovalnih inteligentnih prometnih sistemov (C-ITS); [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610171](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171).

priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje itd.<sup>27</sup>

39. **Posameznik, na katerega se nanašajo osebni podatki**, je fizična oseba, na katero se nanašajo podatki, zajeti z obdelavo. Pri povezanih vozilih so to lahko zlasti voznik (glavni ali občasni), potnik ali lastnik vozila<sup>28</sup>.
40. **Upravljavec podatkov** je oseba, ki določi namene in sredstva obdelave, ki poteka v povezanih vozilih<sup>29</sup>. Upravljavci podatkov lahko vključujejo ponudnike storitev, ki obdelujejo podatke o vozilu, da vozniku pošljejo prometne informacije, sporočila o okolju prijazni vožnji ali opozorila glede delovanja vozila, zavarovalnice, ki ponujajo pogodbe „plačaj, kolikor voziš“, ali proizvajalce vozil, ki zbirajo podatke o obrabi delov vozila za izboljšanje njegove kakovosti. V skladu s členom 26 Splošne uredbe o varstvu podatkov lahko dva ali več upravljavcev skupaj določijo namene in sredstva obdelave in se torej štejejo za skupne upravljavce. V tem primeru morajo jasno opredeliti svoje zadevne obveznosti, zlasti glede uresničevanja pravic posameznikov, na katere se nanašajo osebni podatki, in zagotavljanja informacij, kot so navedene v členih 13 in 14 Splošne uredbe o varstvu podatkov.
41. **Obdelovalec podatkov** je vsaka oseba, ki obdeluje osebne podatke za upravljavca podatkov in v njegovem imenu<sup>30</sup>. Obdelovalec podatkov zbira in obdeluje podatke po navodilu upravljavca podatkov, ne da bi te podatke uporabljal za lastne namene. Proizvajalci opreme in dobavitelji v avtomobilski industriji lahko na primer v številnih primerih podatke obdelujejo v imenu proizvajalcev vozil (kar ne pomeni, da ne morejo biti upravljavci podatkov za druge namene). Poleg tega, da morajo obdelovalci podatkov izvajati ustrezne tehnične in organizacijske ukrepe za zagotovitev ravni varnosti, ki je prilagojena tveganju, člen 28 Splošne uredbe o varstvu podatkov določa obveznosti obdelovalcev podatkov.
42. **Uporabnik** je fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki so mu osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne<sup>31</sup>. Na primer, poslovni partner ponudnika storitve, ki od ponudnika storitve prejme osebne podatke, pridobljene iz vozila, je uporabnik osebnih podatkov. Ne glede na to, ali deluje kot novi upravljavec podatkov ali kot obdelovalec podatkov, mora izpolnjevati vse obveznosti, določene s Splošno uredbo o varstvu podatkov.
43. Vendar pa se javni organi, ki lahko osebne podatke prejmejo v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike<sup>32</sup>; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave. Na primer, organi kazenskega pregona so pooblaščen tretje osebe, kadar zahtevajo osebne podatke v okviru preiskave v skladu s pravom Evropske unije ali države članice.

---

<sup>27</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(2).

<sup>28</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(1).

<sup>29</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(7), in Evropski odbor za varstvo podatkov, Smernice 07/2020 o pojmi upravljavca in obdelovalca v GDPR (v nadaljnjem besedilu: Smernice 07/2020).

<sup>30</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(8), in Smernice 07/2020.

<sup>31</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(9), in Smernice 07/2020.

<sup>32</sup> Splošna uredba o varstvu podatkov, člen 4(9) in uvodna izjava 31.



## 1.5 Tveganja za zasebnost in varstvo podatkov

44. Delovna skupina iz člena 29 je že izrazila več pomislekov glede sistemov interneta stvari, ki lahko veljajo tudi za povezana vozila<sup>33</sup>. Vprašanja glede varnosti podatkov in nadzora, ki so že bila poudarjena glede interneta stvari, so še občutljivejša v okviru povezanih vozil, saj vključujejo pomisleke glede varnosti v cestnem prometu – in lahko vplivajo na telesno celovitost voznika – v okolju, ki se tradicionalno dojema kot izolirano in zaščiteno pred zunanjimi poseganji.
45. Prav tako se pri povezanih vozilih odpirajo precejšnji pomisleki glede varnosti podatkov in zasebnosti v zvezi z obdelavo podatkov o lokaciji, saj lahko njihova čedalje bolj vsiljiva narava obremeni sedanje možnosti za ohranitev anonimnosti. Evropski odbor za varstvo podatkov želi posebno poudariti dejstvo, da uporaba tehnologij za določanje lokacije zahteva izvajanje posebnih zaščitnih ukrepov, da se preprečita nadzor posameznikov in zloraba podatkov, ter okrepi ozaveščenost deležnikov o tem.

### 1.5.1 Pomanjkanje nadzora in informacijska asimetrija

46. Vozniki in potniki v vozilu morda niso vedno ustrezno seznanjeni z obdelavo podatkov, ki poteka v povezanem vozilu ali prek njega. Informacije so morda zagotovljene samo lastniku vozila, ki morda ni voznik, in lahko se zgodi tudi, da niso zagotovljene pravočasno. Zato obstaja tveganje, da ni na voljo dovolj funkcij ali možnosti za izvajanje potrebnega nadzora, da bi lahko prizadeti posamezniki uveljavili svoje pravice glede varstva podatkov in zasebnosti. To je pomembno, saj lahko vozila v svoji življenjski dobi pripadajo več kot enemu lastniku, ker se prodajo ali ker se zakupijo in ne kupijo.
47. Prav tako se lahko komunikacija v vozilu sproži samodejno in tudi po privzeti nastavitvi, ne da bi se posameznik tega zavedal. Ob neobstoju možnosti učinkovitega nadzora nad tem, kako sta vzajemno povezana vozilo in priključena oprema, bo za uporabnika zagotovo postalo izjemno težko nadzorovati tok podatkov. Še težje bo nadzorovati njihovo nadaljnjo uporabo in s tem preprečiti morebitno širitev prvotnega namena.

### 1.5.2 Kakovost uporabnikove privolitve

48. Evropski odbor za varstvo podatkov poudarja, da morajo biti, kadar obdelava podatkov temelji na privolitvi, izpolnjeni vsi elementi veljavne privolitve, kar pomeni, da je privolitev prostovoljna, izrecna in informirana ter pomeni nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, kot je pojasnjeno v smernicah Evropskega odbora za varstvo podatkov o privolitvi<sup>34</sup>. Upravljalci podatkov morajo biti pozorni na načine pridobitve veljavne privolitve od različnih udeležencev, kot so lastniki ali uporabniki avtomobilov. Taka privolitev mora biti dana ločeno za posamezne namene in se ne sme združiti s pogodbo o nakupu ali zakupu novega avtomobila. Privolitev mora biti mogoče tako preprosto preklicati, kot jo je mogoče dati.
49. Enako mora veljati, kadar se privolitev zahteva v skladu z direktivo o e-zasebnosti, na primer pri shranjevanju podatkov ali pridobivanju dostopa do podatkov, že shranjenih v vozilu, kot se v nekaterih primerih zahteva s členom 5(3) direktive o e-zasebnosti. Kot je

---

<sup>33</sup> Delovna skupina iz člena 29 – Mnenje 8/2014 o nedavnem razvoju dogodkov glede interneta stvari; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_sl.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_sl.pdf).

<sup>34</sup> Evropski odbor za varstvo podatkov, Smernice št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, različica 1.1, 4. maj 2020 (v nadaljevanju: Smernice št. 05/2020).

poudarjeno zgoraj, je namreč treba privolitve v tem okviru razlagati po Splošni uredbi o varstvu podatkov.

50. V številnih primerih se uporabnik morda ne zaveda obdelave podatkov, ki poteka v njegovem vozilu. Tako pomanjkanje informacij pomeni veliko oviro za izkaz veljavne privolitve na podlagi Splošne uredbe o varstvu podatkov, saj mora biti privolitev informirana. V takih okoliščinah se na privolitev ni mogoče opreti kot na pravno podlago za ustrezno obdelavo podatkov na podlagi Splošne uredbe o varstvu podatkov.
51. Klasične mehanizme, ki se uporabljajo za pridobitev privolitve posameznikov, bo pri povezanih vozilih morda težko uporabiti, posledica česar je „nekakovostna“ privolitev na podlagi pomanjkanja informacij ali dejanska nezmožnost zagotovitve prilagojene privolitve v skladu s preferencami, ki jih izrazijo posamezniki. V praksi bo privolitev morda težko pridobiti tudi za voznike in potnike, ki niso povezani z lastnikom vozila, v primeru rabljenih, zakupljenih, najetih ali izposojenih vozil.
52. Kadar direktiva o e-zasebnosti ne zahteva privolitve posameznika, na katerega se nanašajo osebni podatki, je upravljavec kljub temu odgovoren, da na podlagi člena 6 Splošne uredbe o varstvu podatkov izbere pravno podlago, ki najbolj ustreza primeru obdelave osebnih podatkov.

### 1.5.3 Nadaljnja obdelava osebnih podatkov

53. Kadar se podatki zberejo na podlagi privolitve, kot se zahteva s členom 5(3) direktive o e-zasebnosti, ali na podlagi ene od izjem iz člena 5(3), in nadalje obdelajo v skladu s členom 6 Splošne uredbe o varstvu podatkov, se lahko nadalje obdelajo le, če upravljavec zaprosi za dodatno privolitev za ta drug namen ali če lahko upravljavec podatkov dokaže, da nadaljnja obdelava temelji na pravu Unije ali države članice za zaščito ciljev iz člena 23(1) Splošne uredbe o varstvu podatkov<sup>35</sup>. Evropski odbor za varstvo podatkov meni, da nadaljnja obdelava na podlagi preizkusa združljivosti v skladu s členom 6(4) Splošne uredbe o varstvu podatkov v takih primerih ni mogoča, ker bi omajala standard varstva podatkov iz direktive o e-zasebnosti. Privolitev, kadar se zahteva na podlagi direktive o e-zasebnosti, mora biti namreč izrecna in informirana, kar pomeni, da morajo biti posamezniki, na katere se nanašajo osebni podatki, seznanjeni z namenom vsake obdelave podatkov in imeti pravico, da zavrnejo določene obdelave<sup>36</sup>. Če bi bila nadaljnja obdelava na podlagi preizkusa združljivosti v skladu s členom 6(4) Splošne uredbe o varstvu podatkov mogoča, bi se s tem zaobšlo samo načelo zahtev glede privolitve, ki jih določa veljavna direktiva.
54. Evropski odbor za varstvo podatkov opozarja, da prvotna privolitev nikoli ne upravičuje nadaljnje obdelave, saj mora biti privolitev informirana in izrecna, da bi bila veljavna.
55. Telemetrični podatki, ki se zbirajo med uporabo vozila za namene vzdrževanja, se na primer zavarovalnicam za motorna vozila ne smejo razkriti brez privolitve uporabnikov za namen oblikovanja profilov voznikov, na podlagi katerih se ponudijo zavarovalne police, ki temeljijo na obnašanju pri vožnji.
56. Poleg tega lahko podatke, ki jih zberejo povezana vozila, obdelajo organi kazenskega pregona za odkrivanje prehitre vožnje ali drugih kršitev, če in ko so izpolnjeni posebni

---

<sup>35</sup> Glej tudi Evropski odbor za varstvo podatkov, Smernice št. 10/2020 o omejitvah na podlagi člena 23 Splošne uredbe o varstvu podatkov.

<sup>36</sup> Smernice št. 05/2020, oddelka 3.2 in 3.3.

pogoji iz direktive o kazenskem pregonu. V tem primeru se bo za take podatke štelo, da se nanašajo na kazenske obsodbe in prekrške pod pogoji iz člena 10 Splošne uredbe o varstvu podatkov in veljavne nacionalne zakonodaje. Proizvajalci lahko organom kazenskega pregona zagotovijo take podatke, če so izpolnjeni posebni pogoji za tako obdelavo. Evropski odbor za varstvo podatkov poudarja, da obdelava osebnih podatkov zgolj za izpolnitev zaprosil organov kazenskega pregona ne pomeni določenega, izrecnega in zakonitega namena v smislu člena 5(1)(b) Splošne uredbe o varstvu podatkov. Kadar so organi kazenskega pregona pooblaščen z zakonom, bi lahko bili tretje osebe v smislu člena 4(10) Splošne uredbe o varstvu podatkov in v takem primeru bi imeli proizvajalci pravico, da jim zagotovijo vse podatke, ki jih imajo na voljo, ob upoštevanju ustreznega pravnega okvira v posamezni državi članici.

#### 1.5.4 Čezmerno zbiranje podatkov

57. Ob čedalje večjem številu senzorjev, nameščenih v povezanih vozilih, obstaja zelo veliko tveganje čezmernega zbiranja podatkov v primerjavi s tem, kar je potrebno za doseg namena.
58. Za razvoj novih funkcionalnosti in natančneje tistih, ki temeljijo na algoritmih strojnega učenja, bo morda potrebna velika količina podatkov, ki se zbirajo v dolgem obdobju.

#### 1.5.5 Varnost osebnih podatkov

59. S številnostjo funkcij, storitev in vmesnikov (na primer splet, USB, RFID, Wi-Fi), ki jih ponujajo povezana vozila, se povečuje prostor za napade in s tem število morebitnih šibkih točk, prek katerih bi bili lahko ogroženi osebni podatki. V nasprotju z večino naprav interneta stvari so povezana vozila kritični sistemi, v katerih lahko kršitev varnosti ogrozi življenje njihovih uporabnikov in ljudi okoli njih. Zato je zelo pomembno obravnavanje tveganja, da bi hakerji poskušali izrabiti šibke točke povezanih vozil.
60. Poleg tega morajo biti osebni podatki, shranjeni v vozilih in/ali na zunanjih lokacijah (na primer infrastrukturah računalništva v oblaku), ustrezno zavarovani pred nepooblaščenim dostopom. Na primer, med vzdrževanjem mora biti vozilo predano tehniku, ki bo zahteval dostop do nekaterih tehničnih podatkov o vozilu. Čeprav mora tehnik imeti dostop do tehničnih podatkov, obstaja možnost, da bi poskušal dostopati do vseh podatkov, shranjenih v vozilu.

## 2 SPLOŠNA PRIPOROČILA

61. Za ublažitev zgoraj opredeljenih tveganj za posameznike, na katere se nanašajo osebni podatki, bi morali proizvajalci vozil in opreme, ponudniki storitev ali drugi deležniki, ki lahko v zvezi s povezanimi vozili delujejo kot upravljavec podatkov ali obdelovalec podatkov, upoštevati naslednja splošna priporočila.

### 2.1 Kategorije podatkov

62. Kot je navedeno v uvodu, se bo večina podatkov, povezanih s povezanimi vozili, štela za osebne podatke, če jih je mogoče povezati z enim ali več določljivimi posamezniki. To vključuje tehnične podatke o gibanju vozila (na primer hitrost, prevožena razdalja) in stanju vozila (na primer temperatura hladilne tekočine motorja, vrtilna frekvenca motorja, tlak v pnevmatikah). Nekaterim podatkom, ki jih ustvarijo povezana vozila, bo morda treba nameniti tudi posebno pozornost zaradi njihove občutljivosti in/ali morebitnega vpliva na



pravice in interese posameznikov, na katere se nanašajo osebni podatki. Evropski odbor za varstvo podatkov je za zdaj opredelil tri kategorije osebnih podatkov, ki jim morajo proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov nameniti posebno pozornost: podatke o lokaciji, biometrične podatke (in katero koli posebno vrsto podatkov, kot je opredeljena v členu 9 Splošne uredbe o varstvu podatkov) in podatke, ki bi lahko razkrivali prekrške ali kršitve v prometu.

### 2.1.1 Podatki o lokaciji

63. Proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov bi morali pri zbiranju osebnih podatkov upoštevati, da podatki o lokaciji še posebno razkrivajo življenjske navade posameznikov, na katere se nanašajo osebni podatki. Opravljene poti so zelo značilne v tem, da omogočajo sklepanje o kraju dela in prebivališča, pa tudi o voznikovih glavnih interesih (prosti čas), ter lahko po možnosti razkrijejo občutljive informacije, na primer veroizpoved prek verskega objekta ali spolno usmerjenost prek krajev, ki jih oseba obiskuje. Proizvajalec vozil in opreme, ponudnik storitev in drug upravljavec podatkov bi zato moral biti posebno pazljiv, da ne zbira podatkov o lokaciji, razen če je to absolutno nujno za namen obdelave. Na primer, kadar obdelava vključuje odkrivanje gibanja vozila, za izpolnitev te funkcije zadostuje žiroskop, ne da bi bilo treba zbirati podatke o lokaciji.

64. Na splošno je treba tudi pri zbiranju podatkov o lokaciji zagotoviti skladnost z naslednjimi načeli:

- Z ustrezna konfiguracija pogostosti dostopa do zbranih podatkov o lokaciji in ravni njihove podrobnosti glede na namen obdelave. Na primer, vremenska aplikacija ne bi smela vsako sekundo dostopati do lokacije vozila, niti s privolitvijo posameznika, na katerega se nanašajo osebni podatki;
- Z zagotovitev natančnih informacij o namenu obdelave (na primer ali je shranjena zgodovina lokacije; če je, kakšen je njen namen);
- Z kadar obdelava temelji na privolitvi, pridobitev veljavne (prostovoljne, izrecne in informirane) privolitve, ki je ločena od splošnih pogojev prodaje ali uporabe, na primer v zvezi z računalnikom v vozilu;
- Z vključitev lokacije šele, ko uporabnik zažene funkcijo, za katero mora biti lokacija vozila znana, in ne kot privzeta nastavitev in vedno ob vžigu avtomobila;
- Z obvestitev uporabnika, da je bila lokacija vključena, zlasti z uporabo ikon (na primer s puščico, ki se premika po zaslonu);
- Z možnost, da se lokacija kadar koli izključi;
- Z opredelitev omejenega obdobja shranjevanja.

### 2.1.2 Biometrični podatki

65. V zvezi s povezanimi vozili se lahko v okviru člena 9 Splošne uredbe o varstvu podatkov in nacionalnih izjem obdelujejo biometrični podatki, ki se uporabljajo za edinstveno identifikacijo posameznika, med drugim, da se omogoči dostop do vozila, avtenticirata voznik oziroma lastnik in/ali omogoči dostop do nastavitev in preferenc v voznikovem profilu. Kadar se razmišlja o uporabi biometričnih podatkov, zagotovitev popolnega nadzora posameznika, na katerega se nanašajo osebni podatki, nad njegovimi podatki

vključuje, na eni strani, zagotovitev obstoja nebiometrične alternative (na primer uporaba fizičnega ključa ali kode) brez dodatne omejitve (tj. uporaba biometrije ne bi smela biti obvezna) in, na drugi strani, shranjevanje in primerjavo biometrične predloge v šifrirani obliki samo lokalno, pri čemer biometričnih podatkov ne obdeluje zunanji terminal za branje oziroma primerjavo.

66. V primeru biometričnih podatkov<sup>37</sup> je pomembno zagotoviti, da je rešitev biometrične avtentikacije dovolj zanesljiva, zlasti z upoštevanjem naslednjih načel:

- Z nastavitvev uporabljenе biometrične rešitve (na primer stopnja lažno pozitivnih in lažno negativnih rezultatov) je prilagojena ravni varnosti zahtevanega nadzora dostopa;
- Z uporabljenа biometrična rešitev temelji na senzorju, ki je odporen proti napadom (kot je uporaba ploskega tiska za prepoznavanje prstnega odtisa);
- Z število poskusov avtentikacije je omejeno;
- Z biometrična predloga oziroma model je shranjen v vozilu v šifrirani obliki z uporabo kriptografskega algoritma in upravljanja s ključi, ki sta v skladu z najsodobnejšo tehnologijo;
- Z surovi podatki, ki se uporabljajo za izdelavo biometrične predloge in avtentikacijo uporabnika, se obdelujejo v realnem času, ne da bi se kadar koli shranili, niti lokalno.

### 2.1.3 Podatki, ki razkrivajo kazniva dejanja ali druge kršitve

67. Za obdelavo podatkov, ki se nanašajo na morebitna kazniva dejanja v smislu člena 10 Splošne uredbe o varstvu podatkov, Evropski odbor za varstvo podatkov priporoča, da se uporabi lokalna obdelava podatkov, pri kateri ima posameznik, na katerega se nanašajo osebni podatki, popolni nadzor nad zadevno obdelavo (glej obravnavo lokalne obdelave v oddelku 2.4). Zunanja obdelava podatkov, ki razkrivajo kazniva dejanja ali druge kršitve, je namreč – razen pri nekaterih izjemah (glej študijo primera o študijah na področju preučevanja in analiziranja vzrokov in posledic nesreč, predstavljeno v oddelku 3.3 spodaj) – prepovedana. Zato je treba glede na občutljivost podatkov uvesti stroge varnostne ukrepe, kot so ukrepi, opisani v oddelku 2.7, da se zagotovi zaščita pred nezakonitim dostopom, spreminjanjem in izbrisom navedenih podatkov.

68. Nekaterе kategorije osebnih podatkov iz povezanih vozil bi dejansko lahko razkrivale, da je bilo ali je storjeno kaznivo dejanje ali kršitev („podatki, povezani s prekrškom“), in bi torej zanje veljale posebne omejitve (na primer podatki, ki kažejo, da je vozilo prevozilo polno črto, trenutna hitrost vozila v povezavi z natančnimi podatki o lokaciji). Zlasti bi se, če bi take podatke obdelali pristojni nacionalni organi za namene kazenske preiskave in pregona kaznivega dejanja, uporabljali zaščitni ukrepi iz člena 10 Splošne uredbe o varstvu podatkov.

## 2.2 Nameni

69. Osebni podatki se lahko obdelujejo za številne različne namene v zvezi s povezanimi vozili, med katerimi so varnost voznika, zavarovanje, učinkovit prevoz, razvedrilne ali informacijske storitve. V skladu s Splošno uredbo o varstvu podatkov morajo upravljavci podatkov zagotoviti, da so njihovi nameni „določeni, izrecni in zakoniti“, da se podatki ne

---

<sup>37</sup> Načelo prepovedi iz člena 9(1) Splošne uredbe o varstvu podatkov se nanaša samo na „biometričn[e] podatk[e] za namene edinstvene identifikacije posameznika“.

obdelujejo nadalje na način, ki ni združljiv s temi nameni, in da obstaja veljavna pravna podlaga za obdelavo, kot se zahteva v členu 5 Splošne uredbe o varstvu podatkov. Nekateri konkretni primeri namenov, ki jih lahko poskušajo doseči upravljavci podatkov v okviru povezanih vozil, so obravnavani v delu III teh smernic, skupaj s konkretnimi priporočili za vsako vrsto obdelave.

### 2.3 Ustreznost in najmanjši obseg podatkov

70. Za upoštevanje načela najmanjšega obsega podatkov<sup>38</sup> bi morali proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov posebno pozornost nameniti kategorijam podatkov, ki jih potrebujejo iz povezanega vozila, saj zbirajo samo osebne podatke, ki so relevantni in potrebni za obdelavo. Podatki o lokaciji so na primer še posebno vsiljivi in lahko razkrivajo številne življenjske navade posameznikov, na katere se nanašajo osebni podatki. Zato bi morali biti udeleženci iz industrije še posebno pazljivi, da ne zbirajo podatkov o lokaciji, razen če je to absolutno nujno za namen obdelave (glej obravnavo podatkov o lokaciji v oddelku 2.1 zgoraj).

### 2.4 Vgrajeno in privzeto varstvo podatkov

71. Ob upoštevanju količine in raznolikosti osebnih podatkov, ki jih proizvajajo povezana vozila, Evropski odbor za varstvo podatkov navaja, da morajo upravljavci podatkov zagotoviti, da so tehnologije, uporabljene v okviru povezanih vozil, konfigurirane tako, da se z uporabo obveznosti vgrajenega in privzetega varstva podatkov, kot se zahteva s členom 25 Splošne uredbe o varstvu podatkov, spoštuje zasebnost posameznikov. Tehnologije bi morale biti zasnovane tako, da se zbira čim manj osebnih podatkov, da so vključene privzete nastavitve za varstvo zasebnosti ter da je zagotovljeno, da so posamezniki, na katere se nanašajo osebni podatki, dobro obveščeni in imajo možnost preprosto spremeniti konfiguracije, povezane z njihovimi osebnimi podatki. Posebne smernice o tem, kako lahko proizvajalci in ponudniki storitev upoštevajo vgrajeno in privzeto varstvo podatkov, bi bile lahko koristne za industrijo in tretje ponudnike aplikacij.

72. K ublažitvi tveganj za pravice in svoboščine posameznikov, povezanih s povezanimi vozili, lahko pripomorejo tudi nekatere splošne prakse, opisane spodaj<sup>39</sup>.

#### 2.4.1 Lokalna obdelava osebnih podatkov

73. Na splošno bi morali proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov, kadar je to mogoče, uporabljati postopke, ki ne vključujejo osebnih podatkov ali prenosa osebnih podatkov zunaj vozila (tj. podatki se obdelujejo interno). Vendar zaradi narave povezanih vozil obstajajo tveganja, kot je možnost napadov na lokalno obdelavo s strani zunanjih akterjev ali uhajanje lokalnih podatkov pri prodaji delov vozila. Zato bi bilo treba ustrezno pozornost nameniti temu, da lokalna obdelava ostane lokalna, in sprejeti varnostne ukrepe za zagotovitev tega. Ta scenarij ponuja prednost, da se uporabniku zagotovi izključni in popolni nadzor nad njegovimi osebnimi podatki, ter kot tak „po zasnovi“ pomeni manj tveganj za zasebnost, zlasti s prepovedjo vsake obdelave podatkov s strani deležnikov brez vednosti posameznika, na katerega se nanašajo osebni podatki. Omogoča tudi obdelavo občutljivih podatkov, kot so biometrični podatki ali podatki v zvezi s kaznivimi dejanji ali drugimi kršitvami, pa tudi podrobnih podatkov o lokaciji, za katere bi

<sup>38</sup> Splošna uredba o varstvu podatkov, člen 5(1)(c).

<sup>39</sup> Glej tudi Evropski odbor za varstvo podatkov, Smernice št. 4/2019 o členu 25 – Vgrajeno in privzeto varstvo podatkov, različica 2.0, sprejete 20. oktobra 2020 (v nadaljevanju: Smernice št. 4/2019).

sicer veljala strožja pravila (glej spodaj). V istem smislu pomeni manj tveganj za kibernetško varnost in vključuje malo latence, zaradi česar je še posebno primeren za avtomatizirane funkcije pomoči pri vožnji. Nekateri primeri take rešitve bi lahko vključevali:

- Z aplikacije za okolju prijazno vožnjo, ki obdelujejo podatke v vozilu za prikaz nasvetov za okolju prijazno vožnjo v realnem času na zaslonu v vozilu;
- Z aplikacije, ki vključujejo prenos osebnih podatkov v napravo, kot je pametni telefon, pod uporabnikovim popolnim nadzorom (na primer prek Bluetootha ali omrežja Wi-Fi), pri čemer se podatki o vozilu ne posredujejo ponudnikom aplikacije ali proizvajalcem vozila; to bi na primer vključevalo priklop pametnih telefonov za uporabo prikazovalnika v avtomobilu, multimedijskih sistemov, mikrofona (ali drugih senzorjev) za telefonske klice itd., če zbrani podatki ostanejo pod nadzorom posameznika, na katerega se nanašajo osebni podatki, in se uporabijo izključno za zagotovitev storitve, ki jo je zahteval;
- Z aplikacije v vozilu za povečanje varnosti, kot so aplikacije, ki oddajajo zvočne signale ali povzročajo vibracije volana, ko voznik prehitava avtomobil, ne da bi to nakazal, ali čez polno črto, ali ki izdajajo opozorila glede stanja vozila (na primer opozorilo o obrabi zavornih ploščic);
- Z aplikacije za odklepanje, vžig in/ali aktiviranje nekaterih ukazov za vozilo, ki uporabljajo voznikove biometrične podatke, shranjene v vozilu (kot so vzorci obraza ali glasu ali podrobnosti prstnega odtisa).

74. Aplikacije, kot so tiste, navedene zgoraj, vključujejo obdelavo, ki jo za izvajanje popolnoma osebnih dejavnosti opravi posameznik (tj. brez prenosa osebnih podatkov upravljavcu podatkov ali obdelovalcu podatkov). Zato v skladu s členom 2(2) Splošne uredbe o varstvu podatkov **te aplikacije ne spadajo na področje uporabe Splošne uredbe o varstvu podatkov.**

75. Če se Splošna uredba o varstvu podatkov ne uporablja za obdelavo osebnih podatkov s strani posameznika v okviru popolnoma osebne ali domače dejavnosti, pa se v skladu z uvodno izjavo 18 Splošne uredbe o varstvu podatkov uporablja za upravljavce ali obdelovalce, ki zagotavljajo sredstva za obdelavo osebnih podatkov za take osebne ali domače dejavnosti (proizvajalci avtomobilov, ponudniki storitev itd.). Kadar torej delujejo kot upravljavec podatkov ali obdelovalec podatkov, morajo razviti varno avtomobilsko aplikacijo ob ustreznem upoštevanju načela vgrajene in privzete zasebnosti. Vsekakor je v uvodni izjavi 78 Splošne uredbe o varstvu podatkov navedeno: „Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi osebnih podatkov ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, bi bilo treba proizvajalce produktov, storitev in aplikacij spodbujati, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja[] zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov“<sup>40</sup>. Po eni strani bo to spodbudilo razvoj na uporabnika naravnanih storitev, po drugi strani pa olajšalo in zaščitilo nadaljnje uporabe v prihodnosti, ki bi lahko spadale na področje uporabe Splošne uredbe o varstvu podatkov. Natančneje, Evropski odbor za varstvo podatkov priporoča razvoj varne platforme za avtomobilске aplikacije, ki je fizično ločena od avtomobilskih funkcij, pomembnih za

---

<sup>40</sup> Za več priporočil o vgrajeni in privzeti zasebnosti glej tudi Smernice št. 4/2019.

varnost, tako da dostop do podatkov o avtomobilu ni odvisen od nepotrebnih zunanjih zmogljivosti v oblaku.

76. Proizvajalci avtomobilov in ponudniki storitev bi morali, kadar koli je to mogoče, premisliti o lokalni obdelavi podatkov, da bi se ublažila morebitna tveganja obdelave v oblaku, kot so poudarjena v mnenju Delovne skupine iz člena 29 o računalništvu v oblaku<sup>41</sup>.

77. Na splošno bi morali imeti uporabniki nadzor nad tem, kako se njihovi podatki zbirajo in obdelujejo v vozilu:

- Z informacije o obdelavi morajo biti zagotovljene v voznikovem jeziku (priročnik, nastavitve itd.);
- Z Evropski odbor za varstvo podatkov priporoča, da se privzeto obdelujejo samo podatki, ki so nujno potrebni za delovanje vozila. Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti možnost vključiti ali izključiti obdelavo podatkov za vsak drug namen in upravljavca oziroma obdelovalca ter imeti možnost izbrisati zadevne podatke ob upoštevanju namena in pravne podlage obdelave podatkov;
- Z podatki se ne bi smeli posredovati tretjim osebam (tj. uporabnik ima izključni dostop do podatkov);
- Z podatki bi se morali hraniti samo tako dolgo, kot je potrebno za opravljanje storitve ali kot se sicer zahteva z zakonodajo Unije ali države članice;
- Z posamezniki, na katere se nanašajo osebni podatki, bi morali imeti možnost trajno izbrisati vse osebne podatke, preden se vozila dajo v prodajo;
- Z posamezniki, na katere se nanašajo osebni podatki, bi morali imeti, kjer je to izvedljivo, neposreden dostop do podatkov, ustvarjenih s temi aplikacijami.

78. Nazadnje, morda ne bo vedno mogoče za vsak primer uporabe uporabiti lokalne obdelave podatkov, je pa pogosto mogoče vzpostaviti „hibridno obdelavo“. Na primer, za zavarovanje na podlagi uporabe bi se lahko osebni podatki v zvezi z obnašanjem pri vožnji (kot je sila, s katero voznik pritiska na zavoro, prepeljeni kilometri) bodisi obdelali znotraj vozila bodisi bi jih v imenu zavarovalnice (upravljavca podatkov) obdelal ponudnik telematskih storitev, da bi ustvaril številčne ocene, ki bi se na opredeljeni podlagi (na primer vsak mesec) prenesle zavarovalnici. Tako zavarovalnica ne pridobi dostopa do surovih podatkov o obnašanju pri vožnji, ampak samo do skupne ocene, ki je rezultat obdelave. To zagotavlja, da so načela najmanjšega obsega podatkov izpolnjena že po zasnovi. To tudi pomeni, da morajo imeti uporabniki možnost uveljavljati svojo pravico, kadar podatke shranjujejo druge strani: uporabnik bi na primer moral imeti možnost, da se pod pogoji iz člena 17 Splošne uredbe o varstvu podatkov izbrišejo podatki, shranjeni v sistemih avtomehanične delavnice ali trgovca z avtomobili.

#### 2.4.2 Anonimizacija in psevdonimizacija

79. Če je predvideno posredovanje osebnih podatkov zunaj vozila, bi bilo treba pred posredovanjem premisliti o njihovi anonimizaciji. Upravljavec bi moral pri anonimizaciji upoštevati vsako zadevno obdelavo, ki bi lahko privedla do deanonimizacije podatkov, kot

---

<sup>41</sup> Delovna skupina iz člena 29 – Mnenje 05/2012 o računalništvu v oblaku; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196\\_sl.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_sl.pdf).

je posredovanje lokalno anonimiziranih podatkov. Evropski odbor za varstvo podatkov opozarja, da se načela varstva podatkov ne uporabljajo za anonimne informacije, tj. informacije, ki niso povezane z določenim ali določljivim posameznikom, ali osebne podatke, ki so bili tako anonimizirani, da posameznik, na katerega se nanašajo osebni podatki, ni ali ni več določljiv<sup>42</sup>. Potem ko je nabor podatkov dejansko anonimiziran in posamezniki niso več določljivi, se evropska zakonodaja o varstvu podatkov ne uporablja več. Posledično je lahko anonimizacija, kjer je ustrezna, dobra strategija za ohranitev koristi povezanih vozil in ublažitev tveganj, povezanih z njimi.

80. Kot je podrobno navedeno v mnenju Delovne skupine iz člena 29 o anonimizacijskih tehnikah, se lahko za anonimizacijo podatkov uporabljajo različne metode, včasih v kombinaciji<sup>43</sup>.
81. Druge tehnike, kot je psevdonimizacija<sup>44</sup>, lahko pomagajo ublažiti tveganja, ki nastanejo z obdelavo podatkov, pri čemer je treba upoštevati, da za doseganje namena obdelave večinoma niso potrebni neposredno določljivi podatki. S psevdonimizacijo se, če je okrepljena z varnostnimi zaščitnimi ukrepi, izboljša varstvo osebnih podatkov tako, da se zmanjšajo tveganja zlorabe. Psevdonimizacija je v nasprotju z anonimizacijo obrnljiva, psevdonimizirani podatki pa se štejejo za osebne podatke, za katere velja Splošna uredba o varstvu podatkov.

#### 2.4.3 Ocene učinka v zvezi z varstvom podatkov

82. Glede na obseg in občutljivost osebnih podatkov, ki se lahko ustvarijo prek povezanih vozil, je verjetno, da bo obdelava – zlasti, kadar se osebni podatki obdelujejo zunaj vozila – pogosto povzročila veliko tveganje za pravice in svoboščine posameznikov. V takem primeru bodo morali udeleženci iz industrije izvesti oceno učinka v zvezi z varstvom podatkov, da bi opredelili in ublažili tveganja, kot je podrobno določeno v členih 35 in 36 Splošne uredbe o varstvu podatkov. Tudi v primerih, v katerih ocena učinka v zvezi z varstvom podatkov ni potrebna, je dobra praksa, da se taka ocena izvede čim prej v procesu zasnove. To bo udeležencem iz industrije omogočilo, da rezultate te analize upoštevajo pri svojih odločitvah o zasnovi pred uvedbo novih tehnologij.

#### 2.5 Informacije

83. Pred obdelavo osebnih podatkov je posameznik, na katerega se nanašajo osebni podatki, obveščen o identiteti upravljavca podatkov (na primer proizvajalec vozil in opreme ali ponudnik storitev), namenu obdelave, uporabnikih podatkov, obdobju hrambe podatkov in pravicah posameznika, na katerega se nanašajo osebni podatki, na podlagi Splošne uredbe o varstvu podatkov<sup>45</sup>.

---

<sup>42</sup> Glej Splošno uredbo o varstvu podatkov, člen 4(1) in uvodna izjava 26.

<sup>43</sup> Delovna skupina iz člena 29 – Mnenje št. 5/2014 o anonimizacijskih tehnikah; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_sl.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sl.pdf).

<sup>44</sup> Splošna uredba o varstvu podatkov, člen 4(5). Poročilo agencije ENISA z dne 3. decembra 2019: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.

<sup>45</sup> Splošna uredba o varstvu podatkov, člen 5(1)(a) in člen 13. Glej tudi Delovna skupina iz člena 29, [Smernice o preglednosti na podlagi Uredbe \(EU\) 2016/679](#), (wp260rev.01), ki jih je potrdil Evropski odbor za varstvo podatkov.

84. Poleg tega bi moral proizvajalec vozil in opreme, ponudnik storitev ali drug upravljavec podatkov posamezniku, na katerega se nanašajo osebni podatki, v jasni, preprosti in zlahka dostopni obliki zagotoviti tudi naslednje informacije:

- Z kontaktne podatke pooblaščenih oseb za varstvo podatkov;
- Z namene, za katere se osebni podatki obdelujejo, in pravno podlago za njihovo obdelavo;
- Z izrecno navedbo zakonitih interesov, ki si jih prizadeva doseči upravljavec ali tretja oseba, kadar taki zakoniti interesi pomenijo pravno podlago za obdelavo;
- Z uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo;
- Z obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- Z obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
- Z obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica, kadar obdelava temelji na privolitvi;
- Z kadar je ustrezno, dejstvo, da namerava upravljavec osebne podatke prenesti v tretjo državo ali mednarodno organizacijo, in zaščitne ukrepe za njihov prenos;
- Z ali je zagotovitev osebnih podatkov zakonska ali pogodbeno obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo;
- Z obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali na podoben način nanj znatno vpliva, ter smiselne informacije o razlogih zanj ter pomenu in predvidenih posledicah take obdelave za posameznika, na katerega se nanašajo osebni podatki. To bi zlasti lahko veljalo pri zagotovitvi zavarovanja na podlagi uporabe za posameznike;
- Z pravico do vložitve pritožbe pri nadzornem organu;
- Z informacije o nadaljnji obdelavi;
- Z v primeru skupnega upravljanja podatkov jasne in popolne informacije o odgovornostih vsakega upravljavca podatkov.

85. V nekaterih primerih se osebni podatki ne zbirajo neposredno pri zadevnem posamezniku. Na primer, proizvajalec vozil in opreme se lahko obrne na trgovca z avtomobili, da bi zbral informacije o lastniku vozila in mu tako ponudil storitev nujne pomoči na cesti. Kadar podatki niso bili zbrani neposredno, proizvajalec vozil in opreme, ponudnik storitev ali drug upravljavec podatkov poleg zgoraj navedenih informacij navede tudi kategorije zadevnih osebnih podatkov, vir, iz katerega so osebni podatki pridobljeni, in, če je ustrezno, ali so bili ti podatki pridobljeni iz javno dostopnih virov. Upravljavec mora navedene informacije

zagotoviti v razumnem roku po pridobitvi podatkov in **najpozneje do prvega od naslednjih datumov** v skladu s členom 14(3) Splošne uredbe o varstvu podatkov: (i) en mesec po pridobitvi podatkov, pri čemer se upoštevajo posebne okoliščine, v katerih se obdelujejo osebni podatki, (ii) ob prvem komuniciranju s posameznikom, na katerega se nanašajo osebni podatki, ali (iii) če se ti podatki posredujejo tretji osebi, pred posredovanjem podatkov.

86. Če posameznike, na katere se nanašajo osebni podatki, prevzame nov upravljavec podatkov, jim bo morda treba zagotoviti tudi nove informacije. Storitve pomoči na cesti, ki je vzajemno povezana s povezanimi vozili, lahko zagotavljajo različni upravljavci podatkov glede na to, v kateri državi ali regiji je potrebna pomoč. Novi upravljavci podatkov bi morali posameznikom, na katere se nanašajo osebni podatki, zagotoviti potrebne informacije, ko posamezniki, na katere se nanašajo osebni podatki, prečkajo meje in novi upravljavci podatkov zagotovijo storitve, ki so vzajemno povezane s povezanimi vozili.
87. Informacije, namenjene posameznikom, na katere se nanašajo osebni podatki, se lahko zagotovijo tudi v delih<sup>46</sup>, tj. z ločitvijo dveh ravni informacij: na eni strani informacije prve ravni, ki so najpomembnejše za posameznike, na katere se nanašajo osebni podatki, in na drugi strani informacije, ki bodo domnevno zanimive pozneje. Bistvene informacije prve ravni poleg identitete upravljavca podatkov vključujejo namen obdelave in opis pravic posameznika, na katerega se nanašajo osebni podatki, ter dodatne informacije o obdelavi, ki najbolj vpliva na posameznika, na katerega se nanašajo osebni podatki, in obdelavi, ki je morda ne pričakuje. Evropski odbor za varstvo podatkov priporoča, da bi morali biti v okviru povezanih vozil posamezniki, na katere se nanašajo osebni podatki, z vsemi uporabniki seznanjeni v prvem delu informacij. Kot je navedeno v smernicah Delovne skupine iz člena 29 o preglednosti, bi morali upravljavci zagotoviti informacije o uporabnikih, ki so za posameznike, na katere se nanašajo osebni podatki, najbolj smiselne. V praksi so to praviloma imenovani uporabniki, tako da posamezniki, na katere se nanašajo osebni podatki, točno vedo, kdo ima njihove osebne podatke. Če upravljavci ne morejo zagotoviti imen uporabnikov, bi morale biti informacije čim bolj podrobne, pri čemer bi bilo treba navesti vrsto uporabnika (tj. s sklicevanjem na dejavnosti, ki jih opravlja), panogo, sektor in podsektor ter lokacijo uporabnikov.
88. Posamezniki, na katere se nanašajo osebni podatki, so lahko obveščeni z jedrnatimi in zlahka razumljivimi določbami v pogodbi o prodaji vozila, pogodbi o opravljanju storitev in/ali katerem koli pisnem mediju z uporabo ločenih dokumentov (na primer servisna knjižica vozila ali priročnik) ali računalnika v vozilu.
89. Poleg potrebnih informacij, kot se zahtevajo na podlagi členov 13 in 14 Splošne uredbe o varstvu podatkov, bi se lahko uporabile standardizirane ikone, da se poveča preglednost, tako da se po možnosti zmanjša potreba po tem, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovijo velike količine informacij v pisni obliki. Te bi morale biti vidne v vozilih, da se na razumljiv in berljiv način zagotovi dober pregled nad načrtovano obdelavo. Evropski odbor za varstvo podatkov poudarja pomen standardizacije navedenih ikon, tako da bo uporabnik videl enake simbole ne glede na znamko ali model vozila. Na primer, kadar vozila zbirajo določene vrste podatkov, kot je lokacija, bi bil lahko

---

<sup>46</sup> Glej Delovna skupina iz člena 29, Smernice o preglednosti na podlagi Uredbe (EU) 2016/679, (wp260rev.01), ki jih je potrdil Evropski odbor za varstvo podatkov.



v njih prikazan jasen signal (kot je lučka v vozilu), s katerim bi bili potniki obveščeni o zbiranju podatkov.

## 2.6 Pravice posameznika, na katerega se nanašajo osebni podatki

90. Proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov bi morali olajšati nadzor posameznikov, na katere se nanašajo osebni podatki, nad njihovimi podatki v celotnem obdobju obdelave z uvedbo posebnih orodij, ki zagotavljajo učinkovit način za uveljavljanje njihovih pravic, zlasti pravice do dostopa, popravka in izbrisa, pravice do omejitve obdelave ter, odvisno od pravne podlage za obdelavo, pravice do prenosljivosti podatkov in pravice do ugovora.
91. Zaradi lažjega spreminjanja nastavitvev bi moral biti uveden sistem upravljanja profila, da bi se shranile preference znanih voznikov in se jim pomagalo, da kadar koli preprosto spremenijo svoje nastavitve zasebnosti. Sistem upravljanja profila bi moral na enem mestu združevati vse nastavitve v zvezi s podatki za vsako obdelavo podatkov, zlasti da se olajša dostop, izbris, odstranitev in prenosljivost osebnih podatkov iz sistemov vozila na zahtevo posameznika, na katerega se nanašajo osebni podatki. Voznikom bi moralo biti omogočeno, da kadar koli začasno ali trajno ustavijo zbiranje nekaterih vrst podatkov, razen če se lahko upravljavec opre na posebno pravno podlago za nadaljevanje zbiranja posebnih podatkov. V primeru pogodbe, ki vsebuje prilagojeno ponudbo na podlagi obnašanja pri vožnji, to lahko pomeni, da bi moral biti uporabnik posledično vrnjen nazaj na standardne pogoje zadevne pogodbe. Te funkcije bi morale biti vključene v vozilo, čeprav bi se lahko posameznikom, na katere se nanašajo osebni podatki, zagotavljale tudi z dodatnimi sredstvi (na primer z namensko aplikacijo). Da se posameznikom, na katere se nanašajo osebni podatki, omogoči, da hitro in preprosto odstranijo osebne podatke, ki se lahko shranijo v armaturni plošči avtomobila (na primer zgodovina navigacije GPS, brskanje po spletu), Evropski odbor za varstvo podatkov poleg tega priporoča, da proizvajalci zagotovijo preprosto funkcijo (kot je na primer gumb za brisanje).
92. Tudi prodaja povezanega vozila in posledična sprememba lastništva bi morali sprožiti izbris vseh osebnih podatkov, ki niso več potrebni za predhodne opredeljene namene, posameznik, na katerega se nanašajo osebni podatki, pa bi moral imeti možnost uveljavljati svojo pravico do prenosljivosti.

## 2.7 Varnost

93. Proizvajalci vozil in opreme, ponudniki storitev in drugi upravljavci podatkov bi morali uvesti ukrepe, ki zagotavljajo varnost in zaupnost obdelanih podatkov, ter sprejeti vse koristne previdnostne ukrepe za preprečitev, da bi nadzor prevzela nepooblaščen oseba. Zlasti bi morali udeleženci iz industrije premisliti o sprejetju naslednjih ukrepov:
- Z šifriranje komunikacijskih poti z najsodobnejšim algoritmom;
  - Z vzpostavitev sistema upravljanja šifrirnih ključev, ki je edinstven za vsako vozilo, ne za vsak model;
  - Z šifriranje podatkov z najsodobnejšimi algoritmi, kadar se shranjujejo na daljavo;
  - Z redno obnavljanje šifrirnih ključev;
  - Z zaščita šifrirnih ključev pred kakršnim koli razkritjem;
  - Z avtentikacija naprav, ki sprejemajo podatke;

- Z zagotavljanje celovitosti podatkov (na primer z zgoščevanjem vsebin);
  - Z pogojevanje dostopa do osebnih podatkov z zanesljivimi tehnikami avtentikacije uporabnika (geslo, elektronsko potrdilo itd.).
94. Kar natančneje zadeva proizvajalce vozil, Evropski odbor za varstvo podatkov priporoča izvajanje naslednjih varnostnih ukrepov:
- Z ločitev ključnih funkcij vozila od funkcij, ki so vedno odvisne od telekomunikacijskih zmogljivosti (na primer informacijsko-razvedrilne funkcije);
  - Z izvajanje tehničnih ukrepov, ki proizvajalcem vozil omogočijo, da hitro odpravijo varnostne pomanjkljivosti v celotni življenjski dobi vozila;
  - Z glede ključnih funkcij vozila čim večje dajanje prednosti uporabi varnih komunikacijskih sredstev, ki so posebej namenjena prevozu;
  - Z vzpostavitev alarmnega sistema v primeru napada na sisteme vozila z možnostjo delovanja v omejenem načinu<sup>47</sup>;
  - Z shranjevanje dnevnika zgodovine vseh dostopov do informacijskega sistema vozila, na primer za največ šest mesecev nazaj, da se omogoči razumevanje izvora morebitnega napada in redno pregledovanje zabeleženih informacij zaradi odkrivanja morebitnih nepravilnosti.
95. Ta splošna priporočila bi bilo treba dopolniti s posebnimi zahtevami ob upoštevanju značilnosti in namena vsake obdelave podatkov.

## 2.8 Posredovanje osebnih podatkov tretjim osebam

96. Načeloma imata dostop do podatkov, ki jih ustvari povezano vozilo, samo upravljavec podatkov in posameznik, na katerega se nanašajo osebni podatki. Vendar lahko upravljavec podatkov osebne podatke posreduje poslovnemu partnerju (uporabniku), kolikor tako posredovanje zakonito temelji na eni od pravnih podlag iz člena 6 Splošne uredbe o varstvu podatkov.
97. Evropski odbor za varstvo podatkov glede na mogočo občutljivost podatkov o uporabi vozila (na primer opravljene poti, slog vožnje) priporoča, da se pred posredovanjem podatkov poslovnemu partnerju, ki deluje kot upravljavec podatkov, sistematično pridobi privolitev posameznika, na katerega se nanašajo osebni podatki (na primer z označitvijo okenca, ki ni vnaprej označeno, ali, kjer je to tehnično mogoče, z uporabo fizične ali logične naprave, do katere lahko oseba dostopa iz vozila). Poslovni partner nato postane odgovoren za podatke, ki jih prejme, in zanj veljajo vse določbe Splošne uredbe o varstvu podatkov.
98. Proizvajalec vozil, ponudnik storitev ali drug upravljavec podatkov lahko osebne podatke posreduje obdelovalcu podatkov, izbranemu za sodelovanje pri zagotovitvi storitve, posamezniku, na katerega se nanašajo osebni podatki, če obdelovalec podatkov navedenih podatkov ne uporabi za lastni namen. Upravljavci podatkov in obdelovalci podatkov

---

<sup>47</sup> Omejen način je način delovanja vozila, ki zagotavlja, da bodo funkcije, ki so nujne za varno delovanje vozila (tj. minimalne varnostne zahteve) delovale, tudi če bodo druge manj pomembne izključene (na primer delovanje naprave za navigacijo se lahko šteje za nebitveno v primerjavi z delovanjem zavornega sistema).

sestavijo pogodbo ali drug pravni dokument, v katerem so podrobno določene obveznosti vsake stranke in predstavljene določbe člena 28 Splošne uredbe o varstvu podatkov.

## 2.9 Prenos osebnih podatkov zunaj EU/EGP

99. Kadar se osebni podatki prenesejo zunaj Evropskega gospodarskega prostora, so predvideni posebni zaščitni ukrepi za zagotovitev, da se z njimi prenese tudi zaščita.
100. Posledično lahko upravljavec podatkov osebne podatke prenese uporabniku le, če je tak prenos v skladu z zahtevami iz poglavja V Splošne uredbe o varstvu podatkov.

## 2.10 Uporaba tehnologij Wi-Fi v vozilu

101. Napredek na področju mobilne tehnologije je omogočil preprosto uporabo interneta na cesti. Čeprav je mogoče povezavo Wi-Fi v vozilu vzpostaviti prek dostopne točke na pametnem telefonu ali posebne naprave (diagnostični vmesnik OBD II, brezžični modem ali usmerjevalnik itd.), večina proizvajalcev danes ponuja modele, ki vključujejo vgrajeno mobilno podatkovno povezavo in so sposobni tudi vzpostaviti omrežja Wi-Fi. Upoštevati je treba različne vidike, ki so odvisni od posameznega primera:

Zpovezavo Wi-Fi kot storitev ponuja poklicni voznik v cestnem prometu, na primer voznik taksija za svoje stranke. V tem primeru bi bilo mogoče poklicnega voznika ali njegovo podjetje šteti za ponudnika internetnih storitev ter bi torej zanj veljale posebne obveznosti in omejitve v zvezi z obdelavo osebnih podatkov njegovih strank;

Zpovezava Wi-Fi je na voljo izključno za voznikovo uporabo (brez voznika in njegovih potnikov). V tem primeru se obdelava osebnih podatkov šteje za popolnoma osebno ali domačo dejavnost v skladu s členom 2(2)(c) in uvodno izjavo 18 Splošne uredbe o varstvu podatkov.

102. Na splošno razširjenost vmesnikov za internetno povezavo prek omrežja Wi-Fi pomeni večja tveganja za zasebnost posameznikov. Uporabniki namreč prek svojih vozil postanejo stalni oddajniki ter jih je torej mogoče določiti in jim slediti. Da bi preprečili sledenje, bi torej morali proizvajalci vozil in opreme uvesti možnosti odklonitve, ki bi bile preproste za uporabo in ki bi zagotavljale, da se ne bi pridobil identifikator nabora storitev (SSID) omrežja Wi-Fi v vozilu.

## 3 ŠTUDIJE PRIMEROV

103. V tem oddelku je obravnavanih pet konkretnih primerov obdelave v okviru povezanih vozil, ki ustrezajo scenarijem, s katerimi se bodo deležniki v sektorju verjetno srečali. Primeri zajemajo obdelavo podatkov, ki zahteva izračun moči, ki ga ni mogoče zagotoviti lokalno v vozilu, in/ali pošiljanje osebnih podatkov tretji osebi za izvedbo nadaljnje analize ali zagotovitev dodatne funkcije na daljavo. Za vsako vrsto obdelave so v tem dokumentu navedeni predvideni nameni, kategorije zbranih podatkov, obdobje hrambe takih podatkov, pravice posameznikov, na katere se nanašajo osebni podatki, varnostni ukrepi, ki jih je treba izvesti, in uporabniki podatkov. Če nekatera od teh področij v nadaljevanju niso opisana, veljajo splošna priporočila, opisana v prejšnjem delu.
104. Izbrani primeri niso izčrpani, njihov namen pa je okvirno predstaviti različne vrste obdelave, pravnih podlag, akterjev itd., ki bi lahko bili vključeni v okvir povezanih vozil.

### 3.1 Zagotavljanje storitve s strani tretje osebe

105. Posamezniki, na katere se nanašajo osebni podatki, lahko s ponudnikom storitev sklenejo pogodbo za pridobitev storitev z dodano vrednostjo glede svojega vozila. Posameznik, na katerega se nanašajo osebni podatki, lahko na primer sklene pogodbo o zavarovanju na podlagi uporabe, ki ponuja znižane zavarovalne premije za manj vožnje („plačaj, kolikor voziš“) ali za dobro obnašanje pri vožnji („plačaj, kakor voziš“), za kar mora zavarovalnica spremljati vozne navade. Posameznik, na katerega se nanašajo osebni podatki, bi tudi lahko sklenil pogodbo s podjetjem, ki ponuja pomoč na cesti v primeru okvare, ki vključuje posredovanje lokacije vozila podjetju, ali s ponudnikom storitve, da bi prejel sporočila ali

opozorila o delovanju vozila (na primer opozorilo o stanju obrabe zavor ali opomnik o datumu tehničnega pregleda).

### 3.1.1 Zavarovanje na podlagi uporabe

106. „Plačaj, kolikor voziš“ je vrsta zavarovanja na podlagi uporabe, pri katerem se spremljajo voznikovo število prevoženih kilometrov in/ali vozne navade, da bi se opredelili in z nižjimi premijami nagradili „varni“ vozniki. Zavarovatelj bo od voznika zahteval, naj namesti vgrajeno telematsko storitev, mobilno aplikacijo ali aktivira vgrajeni modul iz proizvodnje, ki spremlja število prevoženih kilometrov imetnika police in/ali njegovo obnašanje pri vožnji (vzorec zaviranja, hitro pospeševanje itd.). Podatki, zbrani s telematsko napravo, bodo uporabljeni za dodelitev ocen vozniku in analizo, kakšna tveganja lahko ta pomeni za zavarovalnico.
107. Ker je pri zavarovanju na podlagi uporabe potrebna privolitev na podlagi člena 5(3) direktive o e-zasebnosti, Evropski odbor za varstvo podatkov poudarja, da mora imeti imetnik police možnost skleniti zavarovanje, ki ne temelji na uporabi. V nasprotnem primeru se privolitev ne bi štela za prostovoljno, saj bi bilo izvajanje pogodbe pogojeno s privolitvijo. Poleg tega se s členom 7(3) Splošne uredbe o varstvu podatkov zahteva, da mora imeti posameznik, na katerega se nanašajo osebni podatki, pravico preklicati privolitev.

#### 3.1.1.1 Pravna podlaga

108. Kadar se podatki zbirajo prek javno dostopne elektronske komunikacijske storitve (na primer prek kartice SIM v telematski napravi), bo za pridobitev dostopa do podatkov, ki so že shranjeni v vozilu, potrebna privolitev, kot je določeno s členom 5(3) direktive o e-zasebnosti. V tem okviru ni namreč mogoče uporabiti nobene od izjem iz navedenih določb: obdelava se ne izvaja izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja niti ni povezana s storitvijo informacijske družbe, ki jo naročnik ali uporabnik izrecno zahteva. Privolitev bi bilo mogoče pridobiti ob sklenitvi pogodbe.
109. Glede obdelave osebnih podatkov po shranjevanju ali dostopu do terminalne opreme končnega uporabnika se lahko zavarovalnica v tem posebnem okviru opre na člen 6(1)(b) Splošne uredbe o varstvu podatkov, če lahko dokaže, da obdelava poteka v okviru veljavne pogodbe s posameznikom, na katerega se nanašajo osebni podatki, in da je obdelava potrebna za izvajanje konkretne pogodbe s posameznikom, na katerega se nanašajo osebni podatki. Če je obdelava objektivno potrebna za izvajanje pogodbe s posameznikom, na katerega se nanašajo osebni podatki, Evropski odbor za varstvo podatkov meni, da opiranje na člen 6(1)(b) Splošne uredbe o varstvu podatkov v tem konkretnem primeru ne bo zmanjšalo dodatnega varstva, določenega s členom 5(3) direktive o e-zasebnosti. Ta pravna podlaga je konkretizirana s tem, da posameznik, na katerega se nanašajo osebni podatki, podpiše pogodbo z zavarovalnico.

#### 3.1.1.2 Zbrani podatki

110. Upoštevati je treba dve vrsti osebnih podatkov:

**Z komercialne in transakcijske podatke:** identifikacijski podatki posameznika, na katerega se nanašajo osebni podatki, podatki, povezani s transakcijo, podatki o plačilnih sredstvih itd.;

**Z podatke o uporabi:** osebni podatki, ki jih ustvari vozilo, vozne navade, lokacija itd.

111. Evropski odbor za varstvo podatkov priporoča, da se, kolikor je mogoče in glede na tveganje, da bi se lahko podatki, zbrani prek telematske skrinjice, zlorabili za izdelavo natančnega profila voznikovega gibanja, surovi podatki v zvezi z obnašanjem pri vožnji:

Z bodisi obdelajo znotraj vozila v telematskih skrinjicah ali uporabnikovem pametnem telefonu, tako da zavarovatelj dostopa samo do podatkov o rezultatih (na primer ocena glede voznih navad), in ne do podrobnih surovih podatkov (glej oddelek 2.1);

Z bodisi jih obdelata ponudnik telematske storitve v imenu upravljavca (zavarovalnice), da ustvari številčne ocene, ki se na opredeljeni podlagi prenesejo zavarovalnici. V tem primeru je treba ločiti surove podatke in podatke, ki se neposredno nanašajo na identiteto voznika. To pomeni, da ponudnik telematske storitve prejme podatke v realnem času, vendar ne pozna imen, registrskih tablic itd. imetnikov police. Po drugi strani zavarovatelj pozna imena imetnikov police, vendar prejme samo ocene in skupno število kilometrov, in ne surovih podatkov, ki se uporabijo za izdelavo takih ocen.

112. Poleg tega je treba navesti, da se, če je za izvajanje pogodbe potrebno samo število prevoženih kilometrov, podatki o lokaciji ne zbirajo.

#### 3.1.1.3 *Obdobje hrambe*

113. V okviru obdelave podatkov, ki poteka za izvajanje pogodbe (tj. zagotovitev storitve), je pomembno razlikovati med dvema vrstama podatkov, preden se opredelita njuni zadevni obdobji hrambe, in sicer med:

Z **komercialnimi in transakcijskimi podatki**: ti podatki se lahko hranijo v aktivni podatkovni zbirki v celotnem obdobju trajanja pogodbe. Ob koncu pogodbe se lahko arhivirajo fizično (na ločenem mediju: DVD itd.) ali logično (z upravljanjem dovoljenja) za primer morebitnega spora. Nato se po izteku zakonskih zastaralnih rokov podatki izbrišejo ali anonimizirajo;

Z **podatki o uporabi**: podatki o uporabi se lahko razvrstijo kot surovi podatki in zbirni podatki. Kot je navedeno zgoraj, upravljavci ali obdelovalci podatkov ne bi smeli obdelovati surovih podatkov, če je to mogoče. Surove podatke bi bilo treba po potrebi hraniti le tako dolgo, kot je potrebno za izdelavo zbirnih podatkov in preverjanje veljavnosti navedenega postopka združevanja. Zbirne podatke bi bilo treba hraniti tako dolgo, kot je potrebno za opravljanje storitve ali kot se sicer zahteva z zakonodajo Unije ali države članice.

#### 3.1.1.4 *Informacije in pravice posameznikov, na katere se nanašajo osebni podatki*

114. Pred obdelavo osebnih podatkov se posamezniku, na katerega se nanašajo osebni podatki, pregledno in razumljivo zagotovijo informacije v skladu s členom 13 Splošne uredbe o varstvu podatkov. Zlasti ga je treba obvestiti o obdobju hrambe osebnih podatkov ali, če to ni mogoče, merilih, ki se uporabijo za določitev tega obdobja. V zadnje navedenem primeru Evropski odbor za varstvo podatkov priporoča, naj se sprejme pedagoški pristop, da se poudari razlika med surovimi podatki in oceno, izdelano na tej podlagi, pri čemer je treba poudariti, da bo v takem primeru zavarovatelj pridobil samo rezultat ocene, kjer je to ustrezno.

115. Kadar se podatki ne obdelajo znotraj vozila, ampak jih obdelata ponudnik telematske storitve v imenu upravljavca (zavarovalnice), bi bilo v takem primeru v informacijah koristno navesti, da ponudnik ne bo imel dostopa do podatkov, ki se neposredno nanašajo na identiteto voznika (kot so imena, registrske tablice itd.). Prav tako ob upoštevanju pomena obveščanja posameznikov, na katere se nanašajo osebni podatki, glede posledic obdelave

njihovih osebnih podatkov in dejstva, da obdelava osebnih podatkov ne bi smela presenetiti posameznikov, na katere se nanašajo osebni podatki, Evropski odbor za varstvo podatkov priporoča, da bi moral biti posameznik, na katerega se nanašajo osebni podatki, obveščen o obstoju oblikovanja profila in njegovih posledicah, tudi če ne vključuje avtomatiziranega sprejemanja odločitev, kot je navedeno v členu 22 Splošne uredbe o varstvu podatkov.

116. Glede pravice posameznikov, na katere se nanašajo osebni podatki, bodo ti izrecno obveščeni o sredstvih, ki so na voljo za uveljavljanje pravice do dostopa, popravka, omejitve in izbrisa. Ker surove podatke, zbrane v tem okviru, zagotovi posameznik, na katerega se nanašajo osebni podatki (prek posebnih obrazcev ali prek svoje dejavnosti), in se ti obdelajo na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov (izvajanje pogodbe), lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svojo pravico do prenosljivosti podatkov. Kot je poudarjeno v smernicah o pravici do prenosljivosti podatkov, Evropski odbor za varstvo podatkov močno priporoča, „da upravljavci podatkov natančno pojasnijo razliko med vrstami podatkov, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, prejme na podlagi pravice dostopa in pravice do prenosljivosti podatkov“<sup>48</sup>.

117. Informacije se lahko zagotovijo ob podpisu pogodbe.

#### 3.1.1.5 Uporabnik

118. Evropski odbor za varstvo podatkov priporoča, da se, kolikor je mogoče, podatki o uporabi vozila obdelujejo neposredno v telematskih skrinjicah, tako da zavarovatelj dostopa le do podatkov o rezultatih (na primer do ocene), in ne do podrobnih surovih podatkov.

119. Če ponudnik telematskih storitev zbira podatke v imenu upravljavca (zavarovalnica), da izdela številčne ocene, mu ni treba poznati identitete voznika (na primer imen, registrskih tablic itd.), ki je imetnik police.

#### 3.1.1.6 Varnost

120. Veljajo splošna priporočila. Glej oddelek 2.7.

### 3.1.2 Najem in rezervacija parkirnega mesta

121. Lastnik parkirnega mesta bo morda želel parkirno mesto oddati v najem. V ta namen v spletni aplikaciji objavi parkirno mesto in zanj določi ceno. Ko je parkirno mesto uvrščeno v ponudbo, aplikacija obvesti lastnika, ko ga želi voznik rezervirati. Voznik lahko izbere namembni kraj in preveri parkirna mesta, ki so na voljo, na podlagi več meril. Po odobritvi lastnika je transakcija potrjena in ponudnik storitve poskrbi za plačilno transakcijo, nato pa uporabi navigacijo za usmeritev do lokacije.

#### 3.1.2.1 Pravna podlaga

122. Kadar se podatki zbirajo prek javno dostopne elektronske komunikacije, se uporablja člen 5(3) direktive o e-zasebnosti.

123. Ker je to storitev informacijske družbe, se s členom 5(3) direktive o e-zasebnosti ne zahteva privolitev za pridobitev dostopa do podatkov, ki so že shranjeni v vozilu, ko tako storitev izrecno zahteva naročnik.

---

<sup>48</sup> Delovna skupina iz člena 29, Smernice o pravici do prenosljivosti podatkov, WP242 rev.01, potrnil Evropski odbor za varstvo podatkov, str. 13.

124. Za obdelavo osebnih podatkov in samo za podatke, ki so potrebni za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki, bo pravna podlaga člen 6(1)(b).

#### 3.1.2.2 Zbrani podatki

125. Obdelani podatki vključujejo kontaktne podatke voznika (ime, e-naslov, telefonsko številko), vrsto vozila (na primer osebni avtomobil, tovornjak, motorno kolo), registrsko številko, čas parkiranja, podatke o plačilu (na primer podatke o kreditni kartici) in navigacijske podatke.

#### 3.1.2.3 Obdobje hrambe

126. Podatke bi bilo treba hraniti le tako dolgo, kot je potrebno za izpolnitev pogodbe o parkiranju ali kot sicer določa zakonodaja Unije ali države članice. Po tem se podatki bodisi anonimizirajo bodisi izbrišejo.

#### 3.1.2.4 Informacije in pravice posameznikov, na katere se nanašajo osebni podatki

127. Pred obdelavo osebnih podatkov bi bilo treba posamezniku, na katerega se nanašajo osebni podatki, pregledno in razumljivo zagotoviti informacije v skladu s členom 13 Splošne uredbe o varstvu podatkov.
128. Posameznik, na katerega se nanašajo osebni podatki, bi moral biti izrecno obveščen o sredstvih, ki so na voljo, za uveljavljanje svoje pravice do dostopa, popravka, omejitve in izbrisa. Ker podatke, zbrane v tem okviru, zagotovi posameznik, na katerega se nanašajo osebni podatki (prek posebnih obrazcev ali prek svoje dejavnosti), in se ti obdelajo na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov (izvajanje pogodbe), lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svojo pravico do prenosljivosti podatkov. Kot je poudarjeno v smernicah o pravici do prenosljivosti podatkov, Evropski odbor za varstvo podatkov močno priporoča, „da upravljavci podatkov natančno pojasnijo razliko med vrstami podatkov, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, prejme na podlagi pravice dostopa in pravice do prenosljivosti podatkov“.

#### 3.1.2.5 Uporabnik

129. Načeloma imata dostop do podatkov samo upravljavec podatkov in obdelovalec podatkov.

#### 3.1.2.6 Varnost

130. Veljajo splošna priporočila. Glej oddelek 2.7.

### 3.2 eCall

131. V primeru hude nesreče v Evropski uniji vozilo samodejno sproži eCall na številko za klic v sili 112, ki velja po vsej EU (za podrobnosti glej oddelek 1.1), ki omogoča, da se reševalno vozilo takoj pošlje na kraj nesreče v skladu z Uredbo (EU) 2015/758 z dne 29. aprila 2015 o zahtevah za homologacijo za uvedbo sistema eCall, vgrajenega v vozilo, kot storitev številke 112 in spremembi Direktive 2007/46/ES (v nadaljevanju: Uredba (EU) 2015/758).
132. Generator klica eCall, ki je nameščen v vozilo in ki omogoča prenos prek javnega mobilnega brezžičnega komunikacijskega omrežja, začne klic v sili, ki ga bodisi samodejno sprožijo senzorji vozila bodisi ga v primeru nesreče ročno sprožijo potniki v vozilu. Poleg aktivacije avdio kanala je drugi dogodek, ki se ob nesreči samodejno sproži, oblikovanje minimalnega sklopa podatkov, ki se pošlje centru za obveščanje.



### 3.2.1 Pravna podlaga

133. Glede uporabe direktive o e-zasebnosti je treba upoštevati dve določbi:

Z člen 9 v zvezi s podatki o lokaciji, razen podatkov o prometu, ki se uporablja samo za elektronske komunikacijske storitve;

Z člen 5(3) za pridobitev dostopa do podatkov, shranjenih v generatorju, nameščenem v vozilu.

134. Čeprav se s tema določbama načeloma zahteva privolitev posameznika, na katerega se nanašajo osebni podatki, Uredba (EU) 2015/758 pomeni zakonsko obveznost, ki velja za upravljavca podatkov (posameznik, na katerega se nanašajo osebni podatki, nima dejanske ali prostovoljne izbire in ne bo mogel zavrniti obdelave svojih podatkov). Uredba (EU) 2015/758 torej prevlada nad potrebo po voznikovi privolitvi v obdelavo podatkov o lokaciji in minimalnega sklopa podatkov<sup>49</sup>.

135. Pravna podlaga za obdelavo navedenih podatkov bo izpolnitev zakonske obveznosti, kot je določeno v členu 6(1)(c) Splošne uredbe o varstvu podatkov (tj. Uredba (EU) 2015/758).

### 3.2.2 Zbrani podatki

136. Uredba (EU) 2015/758 določa, da podatki, ki se pošljejo s sistemom eCall, vgrajenim v vozilo, kot storitev številke 112, zajemajo samo minimalne informacije iz standarda EN 15722:2015 „Inteligentni transportni sistemi – e-Varnost – Minimalni nabor podatkov za elektronski klic v sili“, ki vključujejo:

Z navedbo, ali je bil eCall sprožen ročno ali samodejno;

Z vrsto vozila;

Z identifikacijsko številko vozila (VIN);

Z tip pogona vozila;

Z časovni žig generiranja prvotnega podatkovnega sporočila v okviru trenutnega dogodka eCall;

Z zadnji znan položaj vozila glede na zemljepisno širino in zemljepisno dolžino, določen v najpoznejšem mogočem trenutku pred generiranjem sporočila;

Z zadnjo znano dejansko smer potovanja vozila, določeno v najpoznejšem mogočem trenutku pred generiranjem sporočila (samo zadnje tri lokacije vozila).

### 3.2.3 Obdobje hrambe

137. Uredba (EU) 2015/758 določa, da se podatki ne hranijo dlje, kot je potrebno za ukrepanje v nujnih primerih. Ko niso več potrebni za ta namen, se vsi ti podatki izbrišejo. Poleg tega se podatki v notranjem spominu sistema eCall samodejno in stalno brišejo. Shranijo se lahko le zadnji trije položaji vozila, če je to nujno potrebno, da se opredelita trenutni položaj in smer vožnje ob dogodku.

---

<sup>49</sup> Navesti je treba, da člen 8(1)(f) pooblastila Sveta za pogajanje za predlog uredbe o „e-zasebnosti“ določa posebno izjemo za eCall, saj privolitev ni potrebna, če „je to potrebno za lociranje terminalne opreme, kadar končni uporabnik v sili naslovi sporočilo na enotno evropsko številko za klic v sili ,112‘ ali na nacionalno številko za klic v sili, v skladu s členom 13(3)“.

### 3.2.4 Informacije in pravice posameznikov, na katere se nanašajo osebni podatki

138. Člen 6 Uredbe (EU) 2015/758 določa, da proizvajalci zagotovijo jasne in popolne informacije o obdelavi podatkov z uporabo sistema eCall. Te informacije se zagotovijo v priložniku za lastnika ločeno za sistem eCall, vgrajen v vozilo, kot storitev številke 112 in vse sisteme eCall, podprte s storitvijo tretje strani, pred uporabo sistema. Te informacije vključujejo:

- Z sklic na pravno podlago za obdelavo;
  - Z dejstvo, da je sistem eCall, vgrajen v vozilo, kot storitev številke 112 privzeto aktiviran;
  - Z postopke obdelave podatkov, ki jih izvaja sistem eCall, vgrajen v vozilo, kot storitev številke 112;
  - Z konkretni namen obdelave klica eCall, omejen na nujne primere iz prvega pododstavka člena 5(2) Uredbe (EU) 2015/758;
  - Z vrste podatkov, ki se zbirajo in obdelujejo, ter prejemnike teh podatkov;
  - Z časovno omejitev hrambe podatkov v sistemu eCall, vgrajenem v vozilo, kot storitev številke 112;
  - Z dejstvo, da vozilo ni predmet stalnega sledenja;
  - Z postopke izvajanja pravic oseb, na katere se nanašajo podatki, in kontaktne službe, pristojne za obravnavo zahtev za dostop;
  - Z druge potrebne dodatne informacije o sledljivosti in sledenju ter obdelavi osebnih podatkov pri zagotavljanju storitve eCall, podprte s storitvijo tretje strani, in/ali drugih storitev z dodano vrednostjo, za kar je potrebno izrecno soglasje lastnika in v skladu s Splošno uredbo o varstvu podatkov. Zlasti je treba upoštevati morebitne razlike med obdelavo podatkov prek sistema eCall, vgrajenega v vozilo, kot storitev številke 112 in sistemov eCall, vgrajenih v vozilo, podprtih s storitvijo tretje strani, ali drugih storitev z dodano vrednostjo.
139. Poleg tega ponudnik storitev posameznikom, na katere se nanašajo osebni podatki, tudi pregledno in razumljivo zagotovi informacije v skladu s členom 13 Splošne uredbe o varstvu podatkov. Posameznik, na katerega se nanašajo osebni podatki, mora biti zlasti obveščen o namenih obdelave osebnih podatkov in dejstvu, da obdelava osebnih podatkov temelji na zakonski obveznosti, ki velja za upravljavca.
140. Poleg tega bi morale biti ob upoštevanju narave obdelave informacije o uporabnikih ali kategorijah uporabnikov osebnih podatkov jasne, posamezniki, na katere se nanašajo osebni podatki, pa bi morali biti obveščeni, da podatki pred sprožitvijo klica eCall niso dostopni nobenemu subjektu zunaj sistema eCall, vgrajenega v vozilo, kot storitev številke 112.
141. Glede pravic posameznikov, na katere se nanašajo osebni podatki, je treba navesti, da se, ker obdelava temelji na zakonski obveznosti, pravica do ugovora in pravica do prenosljivosti ne uporabljata.

### 3.2.5 Uporabnik

142. Podatki pred sprožitvijo klica eCall niso dostopni nobenemu subjektu zunaj sistema eCall, vgrajenega v vozilo, kot storitev številke 112.

143. Sistem eCall ob sprožitvi (bodisi ročni s strani potnikov v vozilu bodisi samodejni, takoj ko senzor v vozilu zazna hudo trčenje) vzpostavi glasovno povezavo z ustreznim centrom za obveščanje in operaterju centra za obveščanje pošlje minimalni sklop podatkov.
144. Poleg tega se lahko podatki, preneseni s sistemom eCall, vgrajenim v vozilo, kot storitev številke 112, ki jih obdelujejo centri za obveščanje, posredujejo službam za ukrepanje ob nesrečah in storitvenim partnerjem iz Sklepa št. 585/2014/EU zgolj ob nesrečah, povezanih s klici eCall, in pod pogoji, določenimi v navedenem sklepu, uporabljajo pa se izključno za doseganje ciljev navedenega sklepa. Podatki, ki jih obdelujejo centri za obveščanje prek sistema eCall, vgrajenega v vozilo, kot storitev številke 112, se brez izrecnega predhodnega soglasja posameznika, na katerega se nanašajo osebni podatki, ne posredujejo nobeni tretji strani.

### 3.2.6 Varnost

145. Uredba (EU) 2015/758 določa zahteve, da se v sistem eCall vgradijo tehnologije za boljše varovanje zasebnosti, da se uporabnikom zagotovijo ustrezna raven varovanja zasebnosti ter potrebni zaščitni ukrepi za preprečevanje nadzоровanja in zlorab. Poleg tega bi morali proizvajalci zagotoviti, da so sistem eCall, ki temelji na številki 112, in vsi drugi sistemi za zagotavljanje sistema eCall, podprtega s storitvijo tretje strani, ali storitve z dodano vrednostjo zasnovani tako, da med njimi ni mogoča izmenjava osebnih podatkov.
146. Glede centrov za obveščanje bi morale države članice zagotoviti, da so osebni podatki zaščiteni pred zlorabo, vključno z nezakonitim dostopom, spreminjanjem ali izgubo, ter da so protokoli o shranjevanju osebnih podatkov, obdobjem hrambe, obdelavo in varstvom določeni na ustrezni ravni in se ustrezno upoštevajo.

### 3.3 Študije na področju preučevanja in analiziranja vzrokov ter posledic nesreč

147. Posamezniki, na katere se nanašajo osebni podatki, lahko prostovoljno privolijo v sodelovanje v študijah na področju preučevanja in analiziranja vzrokov ter posledic nesreč, ki so namenjene boljšemu razumevanju vzrokov nesreč v cestnem prometu in znanstvenim izsledkom na splošno.

#### 3.3.1 Pravna podlaga

148. Kadar se podatki zbirajo prek javne elektronske komunikacijske storitve, bo moral upravljavec podatkov pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki, za dostop do podatkov, ki so že shranjeni v vozilu, kot je določeno s členom 5(3) direktive o e-zasebnosti. V tem okviru ni namreč mogoče uporabiti nobene od izjem iz navedenih določb: obdelava se ne izvaja izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja niti ni povezana s storitvijo informacijske družbe, ki jo naročnik ali uporabnik izrecno zahteva.
149. Glede obdelave osebnih podatkov in ob upoštevanju raznolikosti ter količine osebnih podatkov, potrebnih za študije na področju preučevanja in analiziranja vzrokov in posledic nesreč, Evropski odbor za varstvo podatkov priporoča, naj obdelava temelji na predhodni privolitvi posameznika, na katerega se nanašajo osebni podatki, v skladu s členom 6 Splošne uredbe o varstvu podatkov. Tako predhodno privolitev je treba zagotoviti na posebnem obrazcu, s katerim se posameznik, na katerega se nanašajo osebni podatki, prostovoljno javi za sodelovanje v študiji in strinja z obdelavo njegovih osebnih podatkov za ta namen. Privolitev je prostovoljna, izrecna in informirana izjava volje osebe, katere podatki se obdelujejo (na primer z označitvijo okenca, ki ni vnaprej označeno, ali

konfiguriranjem računalnika v vozilu, da se vključi funkcija v vozilu). Taka privolitev mora biti dana ločeno za posamezne namene in se ne sme združiti s pogodbo o nakupu ali najemu novega avtomobila, poleg tega mora biti privolitev mogoče tako preprosto preklicati, kot jo je mogoče dati. S preklicem privolitve se obdelava ustavi. Podatki se nato iz aktivne podatkovne zbirke izbrišejo ali anonimizirajo.

150. Privolitev, ki se zahteva s členom 5(3) direktive o e-zasebnosti, in privolitev, potrebna kot pravna podlaga za obdelavo podatkov, se lahko pridobita sočasno (na primer z označitvijo okenca, pri katerem je jasno navedeno, v kaj bo privolil posameznik, na katerega se nanašajo osebni podatki).
151. Navesti je treba, da se lahko glede na pogoje obdelave (vrsta upravljavca podatkov itd.) zakonito izbere druga pravna podlaga, če se s tem ne zmanjša dodatno varstvo, določeno s členom 5(3) direktive o e-zasebnosti (glej odstavek 15). Če obdelava temelji na drugi pravni podlagi, kot je opravljanje naloge v javnem interesu (člen 6(1)(e) Splošne uredbe o varstvu podatkov), Evropski odbor za varstvo podatkov priporoča, da se posamezniki, na katere se nanašajo osebni podatki, v študijo vključijo prostovoljno.

### 3.3.2 Zbrani podatki

152. Upravljavec podatkov zbira samo osebne podatke, ki so nujno potrebni za obdelavo.

153. Upoštevati je treba dve vrsti podatkov:

**Z podatke v zvezi z udeleženci in vozili;**

**Z tehnične podatke iz vozil (trenutna hitrost itd.).**

154. Znanstvene raziskave, povezane s preučevanjem in analiziranjem vzrokov in posledic nesreč, upravičujejo zbiranje podatkov o trenutni hitrosti, tudi s strani pravnih oseb, ki ne zagotavljajo javne storitve v strogem pomenu besede.
155. Kot je namreč navedeno zgoraj, Evropski odbor za varstvo podatkov meni, da namen zbiranja podatkov o trenutni hitrosti v okviru študije na področju preučevanja in analiziranja vzrokov ter posledic nesreč ni zbrati podatke, povezane s prekrški (tj. podatki se ne zbirajo za namen preiskave ali pregona prekrška), kar upravičuje njihovo zbiranje s strani pravnih oseb, ki ne zagotavljajo javne storitve v strogem pomenu besede.

### 3.3.3 Obdobje hrambe

156. Pomembno je razlikovati med dvema vrstama podatkov. Prvič, podatki v zvezi z udeleženci in vozili se lahko hranijo za čas trajanja študije. Drugič, tehnične podatke iz vozil bi bilo treba hraniti čim krajši čas, kot je mogoče za namen. V zvezi s tem se zdi pet let od datuma konca študije razumno obdobje. Ob koncu tega obdobja se podatki izbrišejo ali anonimizirajo.

### 3.3.4 Informacije in pravice posameznikov, na katere se nanašajo osebni podatki

157. Pred obdelavo osebnih podatkov se posamezniku, na katerega se nanašajo osebni podatki, pregledno in razumljivo zagotovijo informacije v skladu s členom 13 Splošne uredbe o varstvu podatkov. Zlasti bi morali biti v primeru zbiranja podatkov o trenutni hitrosti posamezniki, na katere se nanašajo osebni podatki, izrecno obveščeni o zbiranju podatkov. Ker obdelava podatkov temelji na privolitvi, mora biti posameznik, na katerega se nanašajo osebni podatki, izrecno obveščen o pravici, da privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave na podlagi privolitve pred njenim preklicem. Poleg tega,

ker podatke, zbrane v tem okviru, zagotovi posameznik, na katerega se nanašajo osebni podatki (prek posebnih obrazcev ali prek svoje dejavnosti), in se ti obdelajo na podlagi člena 6(1)(a) Splošne uredbe o varstvu podatkov (privolitev), lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svojo pravico do prenosljivosti podatkov. Kot je poudarjeno v smernicah o pravici do prenosljivosti podatkov, Evropski odbor za varstvo podatkov močno priporoča, „da upravljavci podatkov natančno pojasnijo razliko med vrstami podatkov, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, prejme na podlagi pravice dostopa in pravice do prenosljivosti podatkov“. Zato bi moral upravljavec podatkov zagotoviti preprost način, da se privolitev prostovoljno in kadar koli prekliče, ter razviti orodja, ki omogočajo odgovor na zahteve za prenosljivost podatkov.

158. Navedene informacije se lahko zagotovijo ob podpisu obrazca o strinjanju s sodelovanjem v študiji na področju preučevanja in analiziranja vzrokov in posledic nesreč.

### 3.3.5 Uporabnik

159. Načeloma imata dostop do podatkov samo upravljavec podatkov in obdelovalec podatkov.

### 3.3.6 Varnost

160. Kot je navedeno zgoraj, se vzpostavljeni varnostni ukrepi prilagodijo ravni občutljivosti podatkov. Na primer, če se v okviru študije na področju preučevanja in analiziranja vzrokov in posledic nesreč zbirajo podatki o trenutni hitrosti (ali kateri koli drugi podatki v zvezi s kazenskimi obsodbami in prekrški), Evropski odbor za varstvo podatkov močno priporoča, da se vzpostavijo strogi varnostni ukrepi, kot so:

- Z izvajanje ukrepov psevdonimizacije (na primer zgoščevanje s tajnim ključem podatkov, kot so priimek/ime posameznika, na katerega se nanašajo osebni podatki, in serijska številka);
- Z shranjevanje podatkov v zvezi s trenutno hitrostjo in lokacijo v ločenih podatkovnih zbirkah (na primer z uporabo najsodobnejšega šifrirnega mehanizma z ločenimi ključi in mehanizmi odobritve);
- Z in/ali izbris podatkov o lokaciji, takoj ko je opredeljen referenčni dogodek ali sekvenca (na primer vrsta ceste, dan/noč), in shranjevanje podatkov, ki omogočajo neposredno identifikacijo, v ločeni podatkovni zbirki, do katere lahko odstopa le majhno število ljudi.

## 3.4 Obravnavanje kraje avtomobila

161. Posamezniki, na katere se nanašajo osebni podatki, bodo morda v primeru kraje poskušali najti svoje vozilo z uporabo lokacije. Uporaba podatkov o lokaciji je omejena zgolj na potrebe preiskave in na oceno zadeve s strani pristojnih pravnih organov.

### 3.4.1 Pravna podlaga

162. Kadar se podatki zbirajo prek javno dostopne elektronske komunikacijske storitve, se uporablja člen 5(3) direktive o e-zasebnosti.
163. Ker je to storitev informacijske družbe, se s členom 5(3) direktive o e-zasebnosti ne zahteva privolitev za pridobitev dostopa do podatkov, ki so že shranjeni v vozilu, ko tako storitev izrecno zahteva naročnik.
164. Kar zadeva obdelavo osebnih podatkov, bo pravna podlaga za obdelavo podatkov o lokaciji privolitev lastnika vozila ali, če je ustrezno, izvajanje pogodbe (samo za podatke, potrebne za izvajanje pogodbe, katere stranka je lastnik vozila).

165. Privolitev je prostovoljna, izrecna in informirana izjava volje osebe, katere podatki se obdelujejo (na primer z označitvijo okenca, ki ni vnaprej označeno, ali konfiguriranjem računalnika v vozilu, da se vključi funkcija v vozilu) Prostovoljna privolitev vključuje možnost, da se privolitev kadar koli prekliče, o čemer bi moral biti posameznik, na katerega se nanašajo osebni podatki, izrecno obveščen. S preklicem privolitve se obdelava ustavi. Podatke bi bilo treba nato izbrisati iz aktivne podatkovne zbirke, anonimizirati ali arhivirati.

#### 3.4.2 Zbrani podatki

166. Podatki o lokaciji se lahko posredujejo šele po prijavi kraje in se v preostalem času ne smejo neprekinjeno zbirati.

#### 3.4.3 Obdobje hrambe

167. Podatki o lokaciji se lahko hranijo le v obdobju, ko zadevo presojuje pristojni pravni organi, ali do konca postopka za odpravo dvoma, ki se ne konča s potrditvijo kraje vozila.

#### 3.4.4 Informacije za posameznike, na katere se nanašajo osebni podatki

168. Pred obdelavo osebnih podatkov bi bilo treba posamezniku, na katerega se nanašajo osebni podatki, pregledno in razumljivo zagotoviti informacije v skladu s členom 13 Splošne uredbe o varstvu podatkov. Natančneje, Evropski odbor za varstvo podatkov priporoča, da upravljavec podatkov poudari, da ni stalnega sledenja vozilu ter da se lahko podatki o lokaciji zberejo in posredujejo šele po prijavi kraje. Poleg tega mora upravljavec posameznika, na katerega se nanašajo osebni podatki, obvestiti, da imajo dostop do podatkov samo pooblaščenim uradnikom platforme za nadzor na daljavo in zakonsko pooblaščenim organom.

169. Kar zadeva pravice posameznikov, na katere se nanašajo osebni podatki, morajo biti ti, kadar obdelava podatkov temelji na privolitvi, izrecno obveščeni o pravici, da privolitev kadar koli prekličejo, ne da bi to vplivalo na zakonitost obdelave na podlagi privolitve pred njenim preklicem. Poleg tega, kadar podatke, zbrane v tem okviru, zagotovijo ti posamezniki (prek posebnih obrazcev ali prek svoje dejavnosti) in se ti obdelajo na podlagi členov 6(1)(a) (privolitev) ali 6(1)(b) Splošne uredbe o varstvu podatkov (izvajanje pogodbe), lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svojo pravico do prenosljivosti podatkov. Kot je poudarjeno v smernicah o pravici do prenosljivosti podatkov, Evropski odbor za varstvo podatkov močno priporoča, „da upravljavci podatkov natančno pojasnijo razliko med vrstami podatkov, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, prejme na podlagi pravice dostopa in pravice do prenosljivosti podatkov“.

170. Zato bi moral upravljavec podatkov zagotoviti preprost način, da se privolitev (samo kadar je privolitev pravna podlaga) prostovoljno in kadar koli prekliče, ter razviti orodja, ki omogočajo odgovor na zahteve za prenosljivost podatkov.

171. Informacije se lahko zagotovijo ob podpisu pogodbe.

#### 3.4.5 Uporabniki

172. V primeru prijave kraje se lahko podatki o lokaciji posredujejo (i) pooblaščenim uradnikom platforme za nadzor na daljavo in (ii) zakonsko pooblaščenim organom.

#### 3.4.6 Varnost

173. Veljajo splošna priporočila. Glej oddelek 2.7.

