Pamatnostādnes 01/2020 par personas datu apstrādi saistībā ar satīklotajiem transportlīdzekļiem un ar mobilitāti saistītām lietotnēm

Versija 2.0

Pieņemtas 2021. gada 9. martā

Versiju vēsture

Versija 2.0	2021. gada 9. martā	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas
Versija 1.0	2020. gada 28. janvārī	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai

Satura rādītājs

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk tekstā — VDAR),

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018[1],

ņemot vērā tās Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1 IEVADS

1. Automobilis — būdams 20. gadsimta ekonomikas simbols — ir viens no masu patēriņa precēm, kas ir ietekmējusi sabiedrību kopumā. Automobiļi, ko mēs parasti saistām ar brīvības jēdzienu, bieži tiek uzskatīti par ko vairāk nekā tikai transportlīdzekli. Patiešām, tie apzīmē privātu zonu, kurā cilvēki var pieņemt autonomus lēmumus bez ārējas iejaukšanās. Mūsdienās, kad satīklotie transportlīdzekļi kļūst par normu, šāds redzējums vairs neatbilst realitātei. Transportlīdzekļu satīklojamība strauji pieaug, sākot no luksusa un augstākās klases modeļiem līdz liela apjoma vidējās klases modeļiem, un transportlīdzekļi kļūst par milzīgiem datu centriem. Arvien vairāk pieaug ne tikai transportlīdzekļu, bet arī autovadītāju un pasažieru satīklojamība. Faktiski daudzos modeļos, kas dažu pēdējo gadu laikā tikuši laisti tirgū, ir integrēti sensori un savienots iebūvēts aprīkojums, kas cita starpā var apkopot un reģistrēt dzinēja darbību, braukšanas paradumus, apmeklētās vietas un potenciāli pat vadītāja acu kustības, viņa pulsu vai biometriskos datus fiziskas personas unikālai identifikācijai.[2]

2. Šāda datu apstrāde notiek sarežģītā ekosistēmā, kas neietver tikai tradicionālos automobiļu rūpniecības dalībniekus, bet ko ietekmē arī jaunu digitālās ekonomikas dalībnieku parādīšanās. Šie jaunie dalībnieki var piedāvāt informācijas un izklaides pakalpojumus, piemēram, tiešsaistes mūziku, informāciju par ceļu stāvokli un satiksmi, vai arī nodrošināt autovadītāja palīdzības sistēmas un pakalpojumus, piemēram, autopilota programmatūru, transportlīdzekļa stāvokļa atjauninājumus, lietojumā balstītu apdrošināšanu vai dinamisko kartēšanu. Turklāt, tā kā transportlīdzekļi ir satīkloti, izmantojot elektroniskos sakaru tīklus, šajā procesā iesaistītajiem ceļu infrastruktūras pārvaldītājiem un telekomunikāciju operatoriem arī ir nozīmīga loma attiecībā uz iespējamām apstrādes darbībām saistībā ar autovadītāju un pasažieru personas datiem.

3. Turklāt satīklotie transportlīdzekļi rada arvien lielāku datu apjomu, no kuriem lielāko daļu var uzskatīt par personas datiem, jo tie attieksies uz autovadītājiem vai pasažieriem. Pat ja tīkla pieslēgtā automobiļa vāktie dati nav tieši saistīti ar vārdu, bet gan ar transportlīdzekļa tehniskajiem aspektiem un elementiem, tie skar automobiļa vadītāju vai pasažierus. Piemēram, dati par braukšanas stilu vai nobraukto attālumu, dati par transportlīdzekļa daļu nodilumu, atrašanās vietas dati vai kameru savāktie dati var attiekties uz autovadītāja uzvedību, kā arī informācija par citiem cilvēkiem, kuri varētu atrasties automobilī, vai datu subjektiem, kas paiet garām. Šādus tehniskos datus rada fiziska persona un ļauj datu

[1] Atsauces uz "dalībvalstīm" šajā dokumentā būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".
[2] Privātuma foruma nākotnes infografika "Dati un tīklam pieslēgts automobilis"; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

pārzinim vai citai personai viņu tieši vai netieši identificēt. Transportlīdzekli var uzskatīt par termināli, kuru var izmantot dažādi lietotāji. Tāpēc, tāpat kā attiecībā uz personālo datoru, šī iespējamā lietotāju daudzveidība neietekmē datu personisko raksturu.

4. 2016. gadā *Fédération Internationale de l'Automobile (FIA)* visā Eiropā rīkoja kampaņu ar nosaukumu "My Car My Data" ("Mana automašīna, mani dati"), lai izpētītu, ko eiropieši domā par tīklam pieslēgtajiem automobiļiem.[3] Lai gan tā parādīja autovadītāju lielo interesi par savienojamību, tā arī uzsvēra, ka uzmanība jāpievērš transportlīdzekļu radīto datu izmantojumam, kā arī to, cik svarīgi ir ievērot personas datu aizsardzības tiesību aktus. Tādējādi katras ieinteresētās personas uzdevums ir iekļaut "personas datu aizsardzības" aspektu jau no izstrādājuma izstrādes posma un nodrošināt automobiļu lietotājiem pārredzamību un kontroli attiecībā uz viņu datiem saskaņā ar VDAR 78. apsvērumu. Šāda pieeja palīdz stiprināt lietotāju uzticību un līdz ar to arī šādu tehnoloģiju ilgtermiņa attīstību.

1.1 Saistītie darbi

5. Satīklotie transportlīdzekļi pēdējās desmitgades laikā ir kļuvuši par nozīmīgu tematu regulatoriem, un pēdējos pāris gados to nozīme ir ievērojami pieaugusi. Tādējādi valstu un starptautiskā līmenī ir publicēti dažādi darbi par satīkloto transportlīdzekļu drošību un privātumu. Šo dokumentu un iniciatīvu mērķis ir papildināt pašreizējos datu aizsardzības un privātuma regulējumus ar nozares noteikumiem vai arī sniegt norādījumus profesionāļiem.

1.1.1 Eiropas līmeņa un starptautiskas iniciatīvas

6. Kopš 2018. gada 31. marta "112" izsaukšanai paredzēta transportlīdzekļa eZvana sistēma ir obligāta visiem jaunajiem M1 un N1 tipa transportlīdzekļiem (vieglajiem pasažieru automobiļiem un vieglajiem transportlīdzekļiem).[4,5] 2006. gadā 29. panta darba grupa jau bija pieņēmusi darba dokumentu par datu aizsardzības un privātuma ietekmi *eCall* iniciatīvā.[6] Turklāt, kā iepriekš ticis apspriests, 29. panta darba grupa 2017. gada oktobrī pieņēma arī atzinumu par personas datu apstrādi sadarbīgu intelektisko transporta sistēmu (S-ITS) kontekstā.

7. Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*) 2017. gada janvārī publicēja pētījumu, kurā galvenā uzmanība tika pievērsta viedo automašīnu kiberdrošībai un noturībai, uzskaitot sensitīvos aktīvus, kā arī atbilstošos draudus, riskus, mazinošos faktorus un iespējamos drošības pasākumus, kas jāīsteno.[7] Starptautiskā datu aizsardzības un privātuma komisāru konference (*ICDPPC*) 2017. gada septembrī pieņēma rezolūciju par satīklotajiem transportlīdzekļiem.[8] Visbeidzot, 2018. gada aprīlī Starptautiskā darba grupa datu aizsardzībai telekomunikāciju jomā (*IWGDPT*) arī pieņēma darba dokumentu par satīklotajiem transportlīdzekļiem.[9]

---

[3] Kampaņa "My Car My Data"; http://www.mycarmydata.eu/.
[4] Sadarbspējīgs ES mēroga *eCall* izsaukums; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Eiropas Parlamenta un Padomes Lēmums Nr. 585/2014/ES (2014. gada 15. maijs) par ES mēroga sadarbspējīgā *eCall* pakalpojuma ieviešanu (Dokuments attiecas uz EEZ) https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32014D0585.
[6] Darba dokuments par datu un privātuma aizsardzību saistībā ar *eCall* iniciatīvu; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_lv.pdf.
[7] Kiberdrošība un viedo automašīnu noturība; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
[8] Rezolūcija par datu aizsardzību automatizētos un satīklotos transportlīdzekļos; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.
[9] Darba dokuments par satīklotajiem transportlīdzekļiem; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.

1.1.2 Eiropas Datu aizsardzības kolēģijas (EDAK) dalībnieku valstu iniciatīvas

8. Vācijas Federālās valsts un federālo zemju datu aizsardzības iestāžu un Vācijas Autobūves nozares asociācijas (VDA) konference 2016. gada janvārī publicēja kopīgu deklarāciju par datu aizsardzības principiem savienotajos un nesavienotos transportlīdzekļos.[10] Apvienotās Karalistes Satīkloto un autonomo transportlīdzekļu centrs (*CCAV*) 2017. gada augustā publicēja rokasgrāmatu, kurā izklāstīti satīkloto un automatizēto transportlīdzekļu kiberdrošības principi, lai vairotu informētību par šo jautājumu automobiļu nozarē.[11] Francijas datu aizsardzības iestāde *Commission Nationale de l'Informatique et des Libertés (CNIL)* 2017. gada oktobrī publicēja atbilstības paketi tīklam pieslēgtajiem automobiļiem, lai palīdzētu ieinteresētajām personām izveidot integrēt datu aizsardzību un datu aizsardzību pēc noklusējuma, dodot iespēju datu subjektiem efektīvi kontrolēt savus datus.[12]

1.2 Piemērojamie tiesību akti

9. Attiecīgais ES tiesiskais regulējums ir VDAR. Tā ir piemērojama visos gadījumos, kad datu apstrāde satīkloto transportlīdzekļu kontekstā ietver sevī indivīdu personas datu apstrādi.

10. Papildus Vispārīgajai datu aizsardzības regulai, Direktīva 2002/58/EK, kas pārskatīta ar Direktīvu 2009/136/EK (turpmāk — "E-privātuma direktīva"), **nosaka īpašu standartu visiem dalībniekiem, kuri vēlas glabāt informāciju vai piekļūt abonenta vai lietotāja informācijai, kas tiek glabāta galiekārtās Eiropas Ekonomikas zonā (EEZ).**

11. Lielākā daļa E-privātuma direktīvas noteikumu (6. pants, 9. pants utt.) attiecas tikai uz publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem un publisko sakaru tīklu nodrošinātājiem, taču E-privātuma direktīvas 5. panta 3. punkts ir vispārīgs noteikums. Tas neattiecas tikai uz elektronisko sakaru pakalpojumiem, bet gan uz visiem subjektiem, gan privātiem, gan publiskiem, kuri izvieto informāciju galiekārtā vai nolasa no tās informāciju neatkarīgi no uzglabājamo vai pieejamo datu rakstura.

12. Jēdziena "galiekārta" (termināliekārta) definīcija ir sniegta Direktīvā 2008/63/EK[13]. 1. panta a) punktā galiekārta definēta kā *"iekārta, ko tieši vai netieši pieslēdz pie publiskā telekomunikāciju tīkla saskarpunkta, lai nosūtītu, apstrādātu vai saņemtu informāciju; abos gadījumos (tieši vai netieši) pieslēgumu var izveidot ar vadiem, optisko šķiedru vai elektromagnētiski; pieslēgums ir netiešs, ja iekārta ir starp termināliekārtu un publiskā telekomunikāciju tīkla saskarpunktu; b) iekārtas ietver arī zemes satelītstaciju iekārtas".*

13. Tā rezultātā, ja ir izpildīti iepriekšminētie kritēriji, satīklotais transportlīdzeklis un tam pievienotā ierīce būtu jāuzskata par "galiekārtu" (tāpat kā datoru, viedtālruni vai viedtelevizoru) un attiecīgā gadījumā piemēro E-privātuma direktīvas 5. panta 3. punktu.

14. Kā norādījusi EDAK savā Atzinumā 5/2019 par E-privātuma direktīvas un VDAR mijiedarbību,[14] E-privātuma direktīvas 5. panta 3. punkts paredz, ka, ievērojot turpmāk 17. punktā minētos šī noteikuma izņēmumus, informācijas uzglabāšanai abonenta vai

---

[10] Datu aizsardzības aspekti satīklotu un nesatīklotu transportlīdzekļu izmantojumā; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.

[11] Kiberdrošības principi satīklotiem un automatizētiem transportlīdzekļiem; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.

[12] Atbilstības pakete atbildīgai datu izmantošanai tīklam pieslēgtos automobiļos; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

[13] Komisijas Direktīva 2008/63/EK (2008. gada 20. jūnijs) par konkurenci telekomunikāciju terminālieākārtu tirgos (Kodificēta versija) (Dokuments attiecas uz EEZ) https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX%3A32008L0063.

[14] Eiropas Datu aizsardzības kolēģija, Atzinums 5/2019 par mijiedarbību starp E-privātuma direktīvu un VDAR jo īpaši attiecībā uz datu aizsardzības iestāžu kompetenci, uzdevumiem un pilnvarām, pieņemts 2019. gada 12. martā (turpmāk — Atzinums 5/2019), 40. punkts.

lietotāja galiekārtā vai piekļuves iegūšanai šādā iekārtā jau uzglabātai informācijai parasti ir nepieciešama iepriekšēja piekrišana. Ja lietotāja galiekārtā uzglabātā informācija satur personas datus, attiecībā uz šīs informācijas uzglabāšanu vai pieejas iegūšanu tai E-privātuma direktīvas 5. panta 3. punkts prevalē pār VDAR 6. pantu.[15] Visām personas datu apstrādes darbībām, kas veiktas pēc iepriekšminētajām apstrādes darbībām, tostarp tādu personas datu apstrādei, kas iegūti, piekļūstot galiekārtas informācijai, ir jābūt juridiskam pamatam atbilstīgi VDAR 6. pantam, lai tās būtu likumīgas.[16]

15. Tā kā pārzinim, lūdzot piekrišanu informācijas uzglabāšanai vai piekļuves iegūšanai šādā iekārtā jau uzglabātai informācijai saskaņā ar E-privātuma direktīvas 5. panta 3. punktu, ir jāinformē datu subjekts par visiem apstrādes nolūkiem, tostarp par jebkādu apstrādi pēc iepriekšminētajām darbībām (proti, "turpmāku apstrādi"), piekrišana atbilstīgi VDAR 6. pantam parasti būs vispiemērotākais juridiskais pamats, lai aptvertu personas datu apstrādi pēc šādām darbībām (ciktāl turpmākās apstrādes nolūku aptver datu subjekta piekrišana, skatīt turpmāk 53.-54. punktu). Tādējādi piekrišana, visticamāk, būs juridiskais pamats gan informācijas uzglabāšanai un piekļuves iegūšanai jau uzglabātai informācijai, gan turpmākajai personas datu apstrādei[17]. Patiešām, novērtējot atbilstību VDAR 6. pantam, jāņem vērā, ka apstrāde kopumā ietver konkrētas darbības, attiecībā uz kurām ES likumdevējs ir centies nodrošināt papildu aizsardzību.[18] Turklāt pārziņiem, nosakot atbilstošo juridisko pamatu, jāņem vērā ietekme uz datu subjektu tiesībām, lai nodrošinātu, ka ir ievērots godprātības princips.[19] Būtībā pārziņi nevar paļauties uz VDAR 6. pantu, lai mazinātu E-privātuma direktīvas 5. panta 3. punktā paredzēto papildu aizsardzību.

16. EDAK atgādina, ka E-privātuma direktīvā lietotais "piekrišanas" jēdziens ir tāds pats kā VDAR lietotais "piekrišanas" jēdziens, un tam jāatbilst visām piekrišanas prasībām, kas paredzētas VDAR 4. panta 11. punktā un 7. pantā.

17. Lai gan principā ir nepieciešama piekrišana, E-privātuma direktīva 5. panta 3. punktā ļauj informācijas uzglabāšanu galiekārtā vai piekļuves iegūšanu šādā iekārtā jau uzglabātai informācijai atbrīvot no informētas piekrišanas prasības, ja tā atbilst kādam no šādiem kritērijiem:

- **Atbrīvojums Nr. 1:** tā paredzēta vienīgi, lai veiktu saziņas pārraidīšanu elektronisko sakaru tīklā;
- **Atbrīvojums Nr. 2:** ja tā noteikti nepieciešama tā informācijas sabiedrības pakalpojuma sniedzējam, kuru skaidri pieprasījis abonents vai lietotājs.

18. Šādos gadījumos personas datu apstrāde, tostarp tādu personas datu, kas iegūti, piekļūstot informācijai galiekārtās, ir balstīta vienā no juridiskajiem pamatiem, kā paredzēts VDAR 6. pantā. Piemēram, piekrišana nav obligāta, ja datu apstrāde ir nepieciešama, lai nodrošinātu GPS navigācijas pakalpojumus, kurus datu subjekts pieprasa, ja šādus pakalpojumus var kvalificēt kā informācijas sabiedrības pakalpojumus.

1.3 Tvērums

19. EDAK vēlas norādīt, ka šīs pamatnostādnes ir paredzētas, lai veicinātu atbilstību saistībā ar personas datu apstrādi, kuru veic plašs šajā vidē strādājošo ieinteresēto personu loks. Tomēr

[15] Turpat, 40. punkts.
[16] Turpat, 41. punkts.
[17] Piekrišanu, kas paredzēta "E-privātuma" direktīvas 5. panta 3. punktā, un piekrišanu, kas nepieciešama kā juridisks pamats datu apstrādei (VDAR 6. pants) vienam un tam pašam konkrētam nolūkam, var iegūt vienlaikus (piemēram, atzīmējot lodziņu, kurā skaidri norādīts, kam datu subjekts piekrīt).
[18] Atzinums 5/2019, 41. punkts.
[19] Eiropas Datu aizsardzības kolēģija, Pamatnostādnes 2/2019 par personas datu apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem, versija 2.0, 2019. gada 8. oktobris, 1. punkts.

tās nav paredzētas, lai aptvertu visus šajā kontekstā iespējamos lietojuma gadījumus vai sniegtu norādījumus par katru iespējamo konkrēto situāciju.

20. Šā dokumenta tvērums ir īpaši vērsts uz personas datu apstrādi saistībā ar to, ka datu subjekti izmanto satīklotus transportlīdzekļus neprofesionālām vajadzībām:: piemēram, autovadītāji, pasažieri, transportlīdzekļu īpašnieki, citi satiksmes dalībnieki utt. Konkrētāk, tas attiecas uz personas datiem: i) ko apstrādā transportlīdzekļa iekšienē, ii) ar ko apmainās transportlīdzeklis un tam pievienotās personīgās ierīces (piemēram, lietotāja viedtālrunis) vai iii) kas tiek vākti lokāli transportlīdzeklī un eksportēti uz ārējām struktūrām (piemēram, transportlīdzekļu ražotājiem, infrastruktūras pārvaldītājiem, apdrošināšanas sabiedrībām, automašīnu remontētājiem) turpmākai apstrādei.

21. Satīklotā transportlīdzekļa definīcija šajā dokumentā ir jāsaprot plaši. To var definēt kā transportlīdzekli, kas aprīkots ar daudziem elektroniskās vadības blokiem (*ECU*), kuri ir savienoti, izmantojot transportlīdzeklī iebūvētu tīklu, kā arī ar savienojamības funkcijām, kas ļauj koplietot informāciju ar citām ierīcēm gan transportlīdzekļa iekšpusē, gan ārpus tā. Tādējādi var apmainīties ar datiem starp transportlīdzekli un tam pieslēgtajām personiskajām ierīcēm, piemēram, ļaujot spoguļot mobilās lietotnes automašīnas paneļa informācijas un izklaides vienībā. Arī atsevišķu mobilo lietotņu, proti, neatkarīgu no transportlīdzekļa (piemēram, paļaujoties tikai uz viedtālruņa lietošanu) izstrāde, lai palīdzētu autovadītājiem, ietilpst šā dokumenta tvērumā, jo tās veicina transportlīdzekļa savienojamības iespējas, lai arī tās nav atkarīgas no datu nosūtīšanas uz transportlīdzekli un no tā. Satīkloto vienoto transportlīdzekļu lietotnes ir daudzas un dažādas, un tās var ietvert turpmāk minētās lietotnes[20].

22. *Mobilitātes pārvaldība:* funkcijas, kas ļauj autovadītājiem ātri un ekonomiski sasniegt galamērķi, savlaicīgi sniedzot informāciju par GPS navigāciju, potenciāli bīstamiem vides apstākļiem (piemēram, apledojušiem ceļiem), satiksmes sastrēgumiem vai ceļu būves darbiem, autostāvvietu vai remontdarbnīcas palīdzību, optimizētu degvielas patēriņu vai autoceļu lietošanas nodevām.

23. *Transportlīdzekļa pārvaldība:* funkcijas, kuru nolūks ir palīdzēt autovadītājiem samazināt ekspluatācijas izmaksas un uzlabot lietošanas ērtumu, piemēram, paziņojums par transportlīdzekļa stāvokli un atgādinājumi par servisu, lietošanas datu nosūtīšana (piemēram, transportlīdzekļu remonta pakalpojumu sniedzējiem), pielāgota apdrošināšana atkarībā no transportlīdzekļa lietojuma, attālinātās darbības (piemēram, apkures sistēma) vai profila konfigurācijas (piemēram, sēdekļa stāvoklis).

24. *Ceļu satiksmes drošība:* funkcijas, kas brīdina autovadītāju par ārējiem apdraudējumiem un iekšējām reakcijām, piemēram, aizsardzība pret sadursmēm, brīdinājumi par bīstamību, brīdinājumi par joslu sadalīšanos, autovadītāja miegainības pakāpes noteikšana, ārkārtas palīdzības izsaukums (*eZvans*) vai avārijas izmeklēšanas "melnās kastes" (notikumu datu reģistrators).

25. *Izklaide:* funkcijas, kas nodrošina informāciju un ietver autovadītāja un pasažieru izklaidi, piemēram, viedtālruņu saskarnes (brīvroku tālruņa zvani, balss ģenerētas īsziņas), *WLAN* karstie punkti, mūzika, video, internets, sociālie mediji, mobilais birojs vai "viedās mājas" pakalpojumi.

26. *Palīdzība autovadītājam:* funkcijas, kas saistītas ar daļēji vai pilnībā automatizētu braukšanu, piemēram, operatīvā palīdzība vai autopilots intensīvas satiksmes apstākļos, stāvvietās vai uz lielceļiem.

[20] *PwC* 2014. gada stratēģija. "In the fast lane. The bright future of connected cars" ("Ātrumjoslā. Tīklam pieslēgto automobiļu spožā nākotne"): https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

27. *Labklājība:* funkcijas, kas kontrolē autovadītāja komfortu, spējas un piemērotību braukšanai, piemēram, noguruma pakāpes noteikšana vai medicīniskā palīdzība.

28. Tādējādi transportlīdzekļi var būt savienoti no sākuma, un personas dati var tikt ievākti, izmantojot vairākus līdzekļus, tostarp: i) transportlīdzekļa sensorus, ii) telemātikas lodziņus vai iii) mobilās lietotnes (piemēram, kurām var piekļūt no ierīces, kas pieder autovadītājam). Lai ietilptu šā dokumenta tvērumā, mobilajām lietotnēm jābūt saistītām ar braukšanas vidi. Piemēram, GPS navigācijas lietotnes ietilpst tvērumā. Šīs pamatnostādnes tomēr neattiecas uz lietotnēm, kuru funkcionalitāte autovadītājiem piedāvā tikai interesējošus objektus (restorānus, vēstures pieminekļus utt.).

29. Liela daļa datu, ko ģenerē satīklotais transportlīdzeklis, attiecas uz fizisku personu, kas ir identificēta vai identificējama, un tādējādi tie ir personas dati. Piemēram, dati ietver tieši identificējamus datus (piemēram, pilnīgu autovadītāja identitāti), kā arī netieši identificējamus datus, piemēram, informāciju par veiktajiem braucieniem, transportlīdzekļa lietošanas datus (piemēram, datus par braukšanas stilu vai nobraukto attālumu) vai transportlīdzekļa tehniskos datus (piemēram, datus par transportlīdzekļa daļu nodilumu), kurus, savstarpēji atsaucoties uz citām datnēm un jo īpaši ar transportlīdzekļa identifikācijas numuru (*VIN*), var saistīt ar fizisku personu. Personas dati satīklotajos transportlīdzekļos var ietvert arī metadatus, piemēram, transportlīdzekļa apkopes statusu. Citiem vārdiem sakot, visi dati, kurus var saistīt ar fizisku personu, tādējādi ietilpst šā dokumenta tvērumā.

30. Satīklotā transportlīdzekļa ekosistēma aptver plašu ieinteresēto personu loku. Konkrētāk, šī ekosistēma ietver tradicionālos automobiļu nozares dalībniekus, kā arī jaunus digitālās nozares dalībniekus. Tādējādi šīs pamatnostādnes ir paredzētas transportlīdzekļu ražotājiem, aprīkojuma ražotājiem un automobiļu piegādātājiem, automašīnu remontētājiem, automašīnu dīleriem, transportlīdzekļu apkopes servisiem, autoparku pārvaldītājiem, transportlīdzekļu apdrošināšanas sabiedrībām, izklaides pakalpojumu sniedzējiem, telesakaru operatoriem, ceļu infrastruktūras pārvaldītājiem un valsts iestādēm, kā arī datu subjektiem. EDAK uzsver, ka datu subjektu kategorijas dažādiem pakalpojumiem atšķirsies (piemēram, autovadītāji, īpašnieki, pasažieri utt.). Šis saraksts nav izsmeļošs, jo ekosistēma ietver plašu pakalpojumu klāstu, tostarp pakalpojumus, kuriem nepieciešama tieša autentifikācija vai identifikācija, un pakalpojumus, kuriem tā nav nepieciešama.

31. Dažas fizisku personu transportlīdzeklī veiktas datu apstrādes darbības ir "tikai personiska vai mājsaimnieciska pasākuma gaitā" veiktas darbības, un tāpēc tās neietilpst VDAR piemērošanas jomā[21]. Tas jo īpaši attiecas uz personas datu izmantošanu transportlīdzekļos, ko veic vienīgie datu subjekti, kuri šādus datus snieguši transportlīdzekļa kontrolmērinstrumentu panelī. Tomēr EDAK atgādina, ka saskaņā ar 18. apsvērumu VDAR "piemēro pārziņiem vai apstrādātājiem, kas nodrošina personas datu apstrādes līdzekļus šādām personiska vai mājsaimnieciska rakstura darbībām".

1.3.1 Šā dokumenta tvērumā neietilpst

32. Darba devēji, kas sava uzņēmuma darbiniekiem nodrošina uzņēmuma automašīnas, varētu vēlēties uzraudzīt sava darbinieka rīcību (piemēram, lai nodrošinātu darbinieka, preču vai transportlīdzekļu drošību, piešķirtu resursus, izsekotu un izrakstītu rēķinu par pakalpojumu vai pārbaudītu darba laiku). Datu apstrāde, ko šajā sakarā veic darba devēji, nodarbinātības kontekstā rada īpašus apsvērumus, ko valsts līmenī var regulēt darba likumi, kurus šajās pamatnostādnēs nevar detalizēti aprakstīt[22].

33. Lai gan datu apstrāde, ko veic saistībā ar komerciāliem transportlīdzekļiem, kurus izmanto profesionāliem nolūkiem (piemēram, sabiedriskais transports), kā arī koplietošanas

[21] Skatīt VDAR, 2. panta 2. punkta c) apakšpunkts.

[22] 29. panta darba grupa šo jautājumu sīkāk aplūkojusi savā WP249 Atzinumā 2/2017 par datu apstrādi darba vietā; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

transportu un *MaaS* risinājumu, var radīt īpašus apsvērumus, kas neietilpst šo vispārīgo pamatnostādņu darbības jomā, daudzi šeit izklāstītie principi un ieteikumi attiecas arī uz šiem apstrādes veidiem.

34. Satīklotie transportlīdzekļi ir ar radio palīdzību iespējotas sistēmas, un uz tiem attiecas pasīvā izsekošana, piemēram, izsekošana ar *Wi-Fi* vai *Bluetooth*. Šajā ziņā tie neatšķiras no citām savienotajām ierīcēm un ietilpst E-privātuma direktīvas, kura pašlaik tiek pārskatīta, piemērošanas jomā. Līdz ar to ir izslēgta arī plaša mēroga ar *Wi-Fi* aprīkotu transportlīdzekļu[23] izsekošana blīvā blakusesošo cilvēku tīklā, kuri izmanto kopīgus viedtālruņu atrašanās vietas noteikšanas pakalpojumus. Tie regulāri ziņo centrālajiem serveriem par visiem redzamajiem *Wi-Fi* tīkliem. Tā kā iebūvēto *Wi-Fi* var uzskatīt par sekundāru transportlīdzekļa identifikatoru[24], tas ietver risku, ka nepārtraukti sistemātiski tiek vākts pilnīgs profils par transportlīdzekļa kustību.

35. Transportlīdzekļi arvien vairāk tiek aprīkoti ar attēlu ierakstīšanas ierīcēm (piemēram, autostāvvietas kameru sistēmām vai paneļu kamerām). Tā kā runa ir par publisku vietu filmēšanu, kam nepieciešams attiecīgā katras dalībvalsts tiesiskā regulējuma novērtējums, šāda datu apstrāde neietilpst šo pamatnostādņu tvērumā.

36. Datu apstrāde, kas nodrošina sadarbīgu intelektisko transporta sistēmu (S-ITS) darbību, kā noteikts Direktīvā 2010/40/ES[25], ir izskatīta īpašā atzinumā, ko izstrādājusi 29. panta darba grupa[26]. Kaut arī S-ITS jēdziena definīcijai direktīvā nav tehnisku specifikāciju, 29. panta darba grupa savā atzinumā galveno uzmanību pievērsa šaura diapazona sakariem, t. i., kas neietver tīkla operatora iejaukšanos. Konkrētāk, tajā sniegta analīze par konkrētiem lietošanas gadījumiem sākotnējā darbības fāzē ar apņemšanos vēlāk izvērtēt jaunos problēmjautājumus, kas neapšaubāmi radīsies, kad tiks ieviests augstāks automatizācijas līmenis. Tā kā ietekme uz datu aizsardzību S-ITS kontekstā ir ļoti specifiska (bezprecedenta atrašanās vietas datu daudzums, nepārtraukta personas datu apraide, datu apmaiņa starp transportlīdzekļiem un citām ceļu infrastruktūras iekārtām utt.) un tā joprojām tiek apspriesta Eiropas līmenī, personas datu apstrāde šajā kontekstā nav aptverta šajās pamatnostādnēs.

37. Visbeidzot, šī dokumenta mērķis nav risināt visas iespējamās problēmas un jautājumus saistībā ar transportlīdzekļiem, un tāpēc to nevar uzskatīt par izsmeļošu.

1.4 Definīcijas

38. Personas datu **apstrāde** ir jebkura darbība, kas ietver personas datus, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana, utt.[27]

[23] Informāciju skatīt: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.

[24] *Markus Ullmann, Tobias Franz* un *Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017,* Sestā starptautiskā konference par transportlīdzekļu sistēmu, tehnoloģiju un lietotņu attīstības sasniegumiem, Nica, Francija, 2017. gada 23.–27. jūlijs, 32.–37. lpp.

[25] Direktīva 2010/40/ES (2010. gada 7. jūlijs) par pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem. https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32010L0040.

[26] 29. panta darba grupas Atzinums 03/2017 par personas datu apstrādi sadarbīgo intelektisko transporta sistēmu (S-ITS) kontekstā: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

[27] Skatīt VDAR, 4. panta 2. punkts.

39. **Datu subjekts** ir fiziska persona, uz kuru attiecas apstrādē ietvertie dati. Satīkloto transportlīdzekļu kontekstā tas jo īpaši var būt autovadītājs (galvenais vai gadījuma rakstura), pasažieris vai transportlīdzekļa īpašnieks.[28]

40. **Datu pārzinis** ir persona, kas nosaka satīklotajos transportlīdzekļos veiktās apstrādes nolūkus un līdzekļus.[29] Datu pārziņi var ietvert pakalpojumu sniedzējus, kuri apstrādā transportlīdzekļa datus, lai nosūtītu autovadītājam informāciju par satiksmi, ekoloģiskas braukšanas ziņojumus vai brīdinājumus par transportlīdzekļa darbību, apdrošināšanas sabiedrības, kas piedāvā uz nobraukumu balstītus ("maksā, kad brauc") līgumus, vai transportlīdzekļu ražotājus, kuri apkopo datus par nolietojumu, kas ietekmē transportlīdzekļa daļas, lai uzlabotu tā kvalitāti. Saskaņā ar VDAR 26. pantu divi vai vairāki pārziņi var kopīgi noteikt apstrādes nolūkus un līdzekļus, un tādējādi tos var uzskatīt par kopīgiem pārziņiem. Šajā gadījumā viņiem ir skaidri jādefinē katra attiecīgie pienākumi, jo īpaši attiecībā uz datu subjektu tiesību izmantošanu un informācijas sniegšanu, kā minēts VDAR 13. un 14. pantā.

41. **Datu apstrādātājs** ir jebkura persona, kas datu pārziņa vārdā un uzdevumā apstrādā personas datus.[30] Datu apstrādātājs apkopo un apstrādā datus saskaņā ar datu pārziņa norādījumiem, neizmantojot šos datus savām vajadzībām. Piemēram, vairākos gadījumos aprīkojuma ražotāji un automobiļu piegādātāji var apstrādāt datus transportlīdzekļu ražotāju vārdā (kas nenozīmē, ka viņi nevar būt datu pārziņi citiem nolūkiem). Papildus prasībai datu apstrādātājiem ieviest atbilstošus tehniskos un organizatoriskos pasākumus, lai garantētu riskam atbilstošu drošības līmeni, VDAR 28. pantā ir izklāstīti datu apstrādātāju pienākumi.

42. **Saņēmējs** ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus — neatkarīgi no tā, vai tā ir trešā persona vai nav.[31] Piemēram, pakalpojumu sniedzēja komerciālais partneris, kurš no pakalpojumu sniedzēja saņem personas datus, kas iegūti no transportlīdzekļa, ir personas datu saņēmējs. Neatkarīgi no tā, vai viņi rīkojas kā jauns datu pārzinis vai kā datu apstrādātājs, viņiem jāievēro visi VDAR noteiktie pienākumi.

43. Tomēr publiskas iestādes, kas var saņemt personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem[32]; minēto datu apstrāde, ko veic minētās publiskās iestādes, atbilst piemērojamiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem. Piemēram, tiesībaizsardzības iestādes ir pilnvarotas trešās personas, ja tās pieprasa personas datus izmeklēšanas ietvaros saskaņā ar Eiropas Savienības vai dalībvalsts tiesību aktiem.

[28] Skatīt VDAR, 4. panta 1. punkts.

[29] Skatīt VDAR 4. panta 7. punktu un Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR (turpmāk — Pamatnostādnes 07/2020).

[30] Skatīt VDAR 4. panta 8. punktu un Pamatnostādnes 07/2020.

[31] Skatīt VDAR 4. panta 9. punktu un Pamatnostādnes 07/2020.

[32] Skatīt VDAR 4. panta 9. punktu un 31. apsvērumu.

1.5 Privātums un datu aizsardzības riski

44. 29. panta darba grupa jau ir paudusi vairākas bažas par lietu interneta (*IoT*) sistēmām, kuras arī var izmantot satīklotajos transportlīdzekļos.[33] Jautājumi par datu drošību un kontroli, kas jau tikuši uzsvērti attiecībā uz *IoT*, ir vēl sensitīvāki satīkloto transportlīdzekļu kontekstā, jo rada bažas par ceļu satiksmes drošību, kā arī var ietekmēt autovadītāja fizisko neaizskaramību vidē, kuru tradicionāli uzskata par izolētu un pasargātu no ārējas iejaukšanās.

45. Arī satīklotie transportlīdzekļi rada ievērojamas bažas attiecībā uz datu aizsardzību un privātumu atrašanās vietas datu apstrādes kontekstā, jo to aizvien uzmācīgākais raksturs var samazināt pašreizējās iespējas palikt anonīmam. EDAK vēlas īpaši uzsvērt un veicināt ieinteresēto personu izpratni par to, ka atrašanās vietas noteikšanas tehnoloģiju izmantošanai ir nepieciešami īpaši drošības pasākumi, lai nepieļautu personu novērošanu un datu ļaunprātīgu izmantošanu.

1.5.1 Kontroles trūkums un informācijas asimetrija

46. Transportlīdzekļu vadītājus un pasažierus ne vienmēr ir iespējams pienācīgi informēt par datu apstrādi, kas tiek veikta satīklotajā transportlīdzeklī vai izmantojot to. Informācija var tikt sniegta tikai transportlīdzekļa īpašniekam, kurš, iespējams, nav autovadītājs, un to var arī nesniegt savlaicīgi. Tādējādi pastāv risks, ka skartajām personām tiek piedāvātas nepietiekamas funkcionalitātes vai iespējas ieviest nepieciešamo kontroli savu datu aizsardzības un privātuma tiesību īstenošanai. Šis punkts ir svarīgs, jo to ekspluatācijas gaitā transportlīdzekļi var piederēt vairākiem īpašniekiem pārdošanas vai arī drīzāk nomas, nevis iegādes, rezultātā.

47. Arī saziņu transportlīdzeklī var aktivizēt automātiski, kā arī pēc noklusējuma, attiecīgajai personai par to neko nezinot. Ja nav iespējas efektīvi kontrolēt transportlīdzekļa un ar to saistītās iekārtas mijiedarbību, lietotājam ir ārkārtīgi grūti kontrolēt datu plūsmu. Būs vēl grūtāk kontrolēt tās turpmāko izmantojumu un tādējādi novērst iespējamo funkciju nesamērīgu pieaugumu.

1.5.2 Lietotāja piekrišanas kvalitāte

48. EDAK uzsver, ka tad, ja datu apstrāde balstās uz piekrišanu, ir jāievēro visi spēkā esošas piekrišanas elementi, kas nozīmē, ka piekrišana ir sniegta brīvi, ir konkrēta un apzināta, un ir nepārprotama norāde uz datu subjekta vēlmēm saskaņā ar interpretāciju EDAK pamatnostādnēs par piekrišanu.[34] Datu pārziņiem ir jāpievērš īpaša uzmanība kārtībai, kā iegūt spēkā esošu piekrišanu no dažādiem dalībniekiem, piemēram, automobiļu īpašniekiem vai automašīnu lietotājiem. Šāda piekrišana ir jāsniedz atsevišķi, konkrētiem nolūkiem, un to nevar apkopot vienā produktā ar jauna automobiļa pirkuma vai līzinga līgumu. Piekrišanas atsaukšanai ir jābūt tikpat vienkāršai kā sniegšanai.

49. Tas pats ir attiecas uz gadījumiem, kad ir nepieciešama piekrišana, lai nodrošinātu atbilstību E-privātuma direktīvai, piemēram, ja notiek informācijas uzglabāšana vai piekļuve transportlīdzeklī jau uzglabātai informācijai, kā noteikts atsevišķos gadījumos saskaņā ar E-privātuma direktīvas 5. panta 3. punktu. Kā minēts iepriekš, piekrišana šajā kontekstā ir jāinterpretē, ņemot vērā VDAR.

50. Daudzos gadījumos lietotājs var nezināt par viņa transportlīdzeklī veikto datu apstrādi. Šāds informācijas trūkums ir būtisks šķērslis spēkā esošas piekrišanas apliecināšanai saskaņā ar

[33] 29. panta darba grupa, Atzinums 8/2014 par jaunākajām tendencēm lietiskā interneta jomā; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_lv.pdf.
[34] Eiropas Datu aizsardzības kolēģija, Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, versija 1.1, 2020. gada 4. maijs (turpmāk — Pamatnostādnes 05/2020).

VDAR, jo piekrišanai jābūt apzinātai. Šādos apstākļos uz piekrišanu nevar atsaukties kā uz juridisko pamatu atbilstošajai datu apstrādei saskaņā ar VDAR.

51. Klasiskos mehānismus, ko izmanto personu piekrišanas iegūšanai, var būt grūti piemērot satīkloto transportlīdzekļu kontekstā, kā rezultātā piekrišana ir "nekvalitatīva", pamatojoties uz informācijas neesību vai faktisku neiespējamību sniegt pielāgotu piekrišanu atbilstoši personu izteiktajām vēlmēm. Lietotu, līzinga, nomātu vai aizņemtu transportlīdzekļu gadījumā piekrišanu no autovadītājiem un pasažieriem, kas nav saistīti ar transportlīdzekļa īpašnieku, praksē var būt grūti saņemt.

52. Ja saskaņā ar E-privātuma direktīvu nav nepieciešama datu subjekta piekrišana, pārzinis jebkurā gadījumā ir atbildīgs par tā juridiskā pamata izvēli saskaņā ar VDAR 6. pantu, kas ir vispiemērotākais personas datu apstrādes gadījumam.

1.5.3 Turpmāka personas datu apstrāde

53. Vācot datus, pamatojoties uz piekrišanu, kā to prasa E-privātuma direktīvas 5. panta 3. punkts vai saskaņā ar kādu no 5. panta 3. punkta izņēmumiem, un pēc tam apstrādājot saskaņā ar VDAR 6. pantu, tos var turpmāk apstrādāt tikai tad, ja pārzinis lūdz papildu piekrišanu šim citam nolūkam vai ja datu pārzinis var pierādīt, ka apstrādes pamatā ir Savienības vai dalībvalsts tiesību akti nolūkā aizsargāt VDAR 23. panta 1. punktā minētos mērķus[35]. EDAK uzskata, ka turpmāka apstrāde, pamatojoties uz saderības pārbaudi atbilstīgi VDAR 6. panta 4. punktam, šādos gadījumos nav iespējama, jo tas grautu E-privātuma direktīvas datu aizsardzības standartu. Piekrišanai, ja to prasa E-privātuma direktīva, ir jābūt konkrētai un apzinātai, kas nozīmē, ka datu subjektiem ir jāzina ikviens datu apstrādes nolūks un viņiem ir tiesības atteikties no apstrādes konkrētiem nolūkiem[36]. Uzskatot, ka turpmāka apstrāde, pamatojoties uz saderības pārbaudi saskaņā ar VDAR 6. panta 4. punktu, ir iespējama, tiktu apiets pašreizējā direktīvā noteikto piekrišanas prasību princips.

54. EDAK atgādina, ka sākotnējā piekrišana nekādā gadījumā nepadara likumīgu turpmāku apstrādi, jo piekrišanai, lai tā būtu spēkā esoša, jābūt apzinātai un konkrētai.

55. Piemēram, telemetrijas datus, kas tiek savākti transportlīdzekļa lietojuma gaitā tehniskās apkopes vajadzībām, nedrīkst izpaust transportlīdzekļu apdrošināšanas sabiedrībām bez lietotāju piekrišanas, lai izveidotu autovadītāju profilus nolūkā piedāvāt braukšanas uzvedībā balstītas apdrošināšanas polises.

56. Turklāt tiesībaizsardzības iestādes var apstrādāt datus, kas savākti, izmantojot satīklotos transportlīdzekļus, lai konstatētu ātruma pārsniegšanu vai citus pārkāpumus, ja un kad ir izpildīti tiesībaizsardzības direktīvas īpašie nosacījumi. Šajā gadījumā šādi dati tiks uzskatīti par saistītiem ar notiesājošiem spriedumiem un nodarījumiem atbilstīgi VDAR 10. pantā un visos piemērojamos valsts tiesību aktos noteiktajiem nosacījumiem. Ražotāji var sniegt tiesībaizsardzības iestādēm šādus datus, ja ir izpildīti īpaši apstrādes nosacījumi. EDAK norāda, ka personas datu apstrāde tikai un vienīgi tiesībaizsardzības iestāžu pieprasījumu izpildei nav konkrēts, skaidrs un leģitīms nolūks VDAR 5. panta 1. punkta b) apakšpunkta izpratnē. Ja tiesībaizsardzības iestādes ir pilnvarotas saskaņā ar likumu, tās var būt trešās personas VDAR 4. panta 10. punkta izpratnē, un šajā gadījumā ražotājiem būtu tiesības sniegt viņiem visus to rīcībā esošos datus, ievērojot katras dalībvalsts attiecīgo tiesisko regulējumu.

[35] Skatīt Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu.
[36] Pamatnostādnes 05/2020, 3.2. un 3.3. sadaļa.

1.5.4 Pārmērīga datu vākšana

57. Tā kā satīklotajos transportlīdzekļos izvieto arvien lielāku sensoru skaitu, pastāv ļoti liels pārmērīgas datu vākšanas risks, salīdzinot ar to, kas nepieciešams mērķa sasniegšanai.

58. Lai izstrādātu jaunas funkcionalitātes un, konkrētāk, tādas, kuras balstītas mašīnmācīšanās algoritmos, var būt nepieciešams ilgākā laikposmā savākts liels datu daudzums.

1.5.5 Personas datu drošība

59. Satīkloto transportlīdzekļu piedāvātās daudzās funkcionalitātes, pakalpojumi un saskarnes (piemēram, tīmeklis, *USB, RFID, Wi-Fi)* palielina uzbrukuma tvērumu un līdz ar to iespējamo ievainojamību skaitu, ar kuru starpniecību var tikt apdraudēti personas dati. Atšķirībā no vairuma *IoT* ierīču satīklotie transportlīdzekļi ir kritiski svarīgas sistēmas, kuru drošības pārkāpums var apdraudēt tā lietotāju un apkārtējo cilvēku dzīvību. Tādējādi kļūst vēl būtiskāk apkarot risku, ka datorpirāti mēģina izmantot satīkloto transportlīdzekļu ievainojamību..

60. Turklāt transportlīdzekļos un/vai ārējās vietās (piemēram, mākoņdatošanas infrastruktūrās) uzglabātie personas dati ir atbilstoši jāaizsargā pret neatļautu piekļuvi. Piemēram, apkopes laikā transportlīdzeklis jānodod tehniķim, kuram būs nepieciešama piekļuve noteiktiem transportlīdzekļa tehniskajiem datiem. Kaut arī tehniķim ir nepieciešama piekļuve tehniskajiem datiem, pastāv iespēja, ka viņš varētu mēģināt piekļūt visiem transportlīdzeklī uzglabātajiem datiem.

2 VISPĀRĪGI IETEIKUMI

61. Lai mazinātu iepriekš identificētos riskus datu subjektiem, transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem vai jebkurai citai ieinteresētajai personai, kas var darboties kā datu pārzinis vai datu apstrādātājs saistībā ar satīklotajiem transportlīdzekļiem, būtu jāievēro šādi vispārīgi ieteikumi.

2.1 Datu kategorijas

62. Kā atzīmēts ievadā, lielākā daļa ar satīklotajiem transportlīdzekļiem saistīto datu tiks uzskatīti par personas datiem tiktāl, ciktāl tos ir iespējams saistīt ar vienu vai vairākām identificējamām personām. Tas ietver tehniskos datus par transportlīdzekļa kustību (piemēram, ātrumu, nobraukto attālumu), kā arī par transportlīdzekļa stāvokli (piemēram, motora dzesēšanas šķidruma temperatūra, motora apgriezienu skaits, spiediens riepās). Atsevišķiem satīkloto transportlīdzekļu ģenerētajiem datiem var arī būt nepieciešama īpaša uzmanība, ņemot vērā to sensitivitāti un/vai iespējamo ietekmi uz datu subjektu tiesībām un interesēm. Pašlaik EDAK ir noteikusi trīs personas datu kategorijas, kurām jāpievērš īpaša uzmanība — transportlīdzekļu un aprīkojuma ražotāji, pakalpojumu sniedzēji un citi datu pārziņi: atrašanās vietas dati, biometriskie dati (un jebkura īpaša datu kategorija, kā noteikts VDAR 9. pantā) un dati, kas varētu atklāt noziedzīgus nodarījumus vai satiksmes pārkāpumus.

2.1.1 Atrašanās vietas dati

63. Vācot personas datus, transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem un citiem datu pārziņiem būtu jāpatur prātā, ka atrašanās vietas dati jo īpaši atklāj datu subjektu sadzīves paradumus. Veiktie braucieni ir ļoti raksturīgi, jo tie ļauj konstatēt darba vietu un dzīvesvietu, kā arī autovadītāja interešu jomas (brīvā laika pavadīšanu) un, iespējams, izpaust sensitīvu informāciju, piemēram, reliģisko pārliecību ar lūgšanu nama starpniecību, vai informāciju par seksuālo orientāciju, pamatojoties uz apmeklētajām vietām. Attiecīgi transportlīdzekļa un aprīkojuma ražotājam, pakalpojumu sniedzējam un citam datu pārzinim vajadzētu būt īpaši piesardzīgiem un nevākt atrašanās vietas datus, izņemot gadījumus, kad tas ir absolūti nepieciešams apstrādes nolūkā.

Piemēram, ja apstrāde ir transportlīdzekļa kustības noteikšana, šīs funkcijas izpildei pietiek ar žiroskopu, un nav nepieciešams vākt atrašanās vietas datus.

64. Uz atrašanās vietas datu vākšanu parasti attiecas arī šādi principi:

- adekvāta piekļuves biežuma un vākto atrašanās vietas datu detalizācijas līmeņa konfigurācija attiecībā pret apstrādes nolūku. Piemēram, laika apstākļu lietotnei nedrīkstētu būt iespēja piekļūt transportlīdzekļa atrašanās vietai ik sekundi pat ar datu subjekta piekrišanu;
- precīzas informācijas sniegšana par apstrādes nolūku (piemēram, vai tiek saglabāta atrašanās vietu vēsture? Ja tā ir, kāds ir nolūks?);
- ja apstrādes pamatā ir piekrišana, spēkā esošas (brīvas, konkrētas un apzinātas) piekrišanas iegūšana atsevišķi no vispārējiem pārdošanas vai lietošanas nosacījumiem, piemēram, iebūvētajā datorā;
- atrašanās vietas aktivizēšana tikai tad, kad lietotājs iedarbina funkciju, kurai nepieciešama transportlīdzekļa atrašanās vietas informācija, nevis pēc noklusējuma un nepārtraukti, kad automašīna tiek iedarbināta;
- lietotāja informēšana par atrašanās vietas informācijas aktivizēšanu, jo īpaši izmantojot ikonas (piemēram, bultiņu, kas pārvietojas pa ekrānu);
- iespēja jebkurā laikā deaktivizēt atrašanās vietu;
- ierobežota glabāšanas termiņa noteikšana.

2.1.2 Biometriskie dati

65. Satīkloto transportlīdzekļu kontekstā biometriskos datus, ko izmanto fiziskas personas unikālai identificēšanai, var apstrādāt VDAR 9. panta un valstu noteiktu izņēmumu ietvaros, cita starpā, lai nodrošinātu piekļuvi transportlīdzeklim, lai autentificētu autovadītāju/īpašnieku un/vai lai piekļūtu autovadītāja profila iestatījumiem un vēlmēm. Apsverot biometrisko datu izmantošanu, kas garantētu datu subjektam pilnīgu kontroli pār saviem datiem, no vienas puses, ir jānodrošina alternatīva, kas nav biometriska (piemēram, fiziskas atslēgas vai koda izmantošana) bez papildu ierobežojumiem (tas ir, biometrisko datu lietošanai nevajadzētu būt obligātai), un, no otras puses, biometriskās veidnes glabāšana un salīdzināšana šifrētā veidā tikai lokāli, neapstrādājot biometriskos datus ar ārēju lasīšanas/salīdzināšanas terminālu palīdzību.

66. Biometrisko datu[37] gadījumā ir svarīgi nodrošināt, ka biometriskās autentifikācijas risinājums ir pietiekami uzticams, jo īpaši ievērojot šādus principus:

- izmantotā biometriskā risinājuma korekcija (piemēram, viltus pozitīvs un viltus negatīvs rādītājs) tiek pielāgota vajadzīgās piekļuves kontroles drošības līmenim;
- izmantotā biometriskā risinājuma pamatā ir sensors, kas ir noturīgs pret uzbrukumiem (piemēram, plakanās drukas izmantošana pirkstu nospiedumu atpazīšanai);
- autentifikācijas mēģinājumu skaits ir ierobežots;
- biometriskā veidne/modelis tiek uzglabāts transportlīdzeklī šifrētā veidā, izmantojot kriptogrāfisko algoritmu un atslēgu pārvaldību, kas atbilst jaunākajiem tehnikas sasniegumiem;
- neapstrādātie dati, ko izmanto biometriskās veidnes izveidē un lietotāju autentifikācijai, tiek apstrādāti reāllaikā, tos nekādā gadījumā neglabājot pat lokāli.

[37] VDAR 9. panta 1. punktā noteiktais aizlieguma princips attiecas tikai uz "biometriskiem datiem, lai veiktu fiziskas personas unikālu identifikāciju".

2.1.3 Dati, kas atklāj noziedzīgus nodarījumus vai citus pārkāpumus

67. Lai apstrādātu datus, kas attiecas uz iespējamiem noziedzīgiem nodarījumiem VDAR 10. panta izpratnē, EDAK iesaka izmantot vietēju datu apstrādi, kad datu subjektam ir pilnīga kontrole pār attiecīgo apstrādi (skatīt vietējās apstrādes apspriešanu 2.4. iedaļā). Patiešām, atskaitot dažus izņēmumus (skatīt konkrētos piemērus negadījumu pētījumiem turpmāk 3.3. iedaļā), datu ārēja apstrāde, kas atklāj noziedzīgus nodarījumus vai citus pārkāpumus, ir aizliegta. Tādējādi, ņemot vērā datu sensitivitāti, jāievieš stingri drošības pasākumi, piemēram, 2.7. iedaļā aprakstītie, lai nodrošinātu aizsardzību pret nelikumīgu piekļuvi šādiem datiem, to pārveidi un dzēšanu.

68. Patiešām, dažu kategoriju personas dati no satīklotajiem transportlīdzekļiem var atklāt, ka ir vai tiek izdarīts noziedzīgs nodarījums vai cits pārkāpums ("ar noziedzīgiem nodarījumiem saistīti dati"), un tāpēc uz tiem attiecas īpaši ierobežojumi (piemēram, dati, kas norāda, ka transportlīdzeklis šķērsojis balto līniju, transportlīdzekļa momentānais ātrums apvienojumā ar precīziem atrašanās vietas datiem). Jo īpaši, ja šādus datus valsts kompetentās iestādes apstrādā kriminālizmeklēšanas un kriminālvajāšanas nolūkā, būtu jāpiemēro VDAR 10. pantā paredzētās garantijas.

2.2 Nolūki

69. Personas datus var apstrādāt dažādiem nolūkiem saistībā ar satīklotajiem transportlīdzekļiem, tostarp autovadītāja drošības, apdrošināšanas, efektīvas transportēšanas, izklaides vai informācijas pakalpojumu nolūkiem. Saskaņā ar VDAR datu pārziņiem ir jānodrošina, lai viņu nolūki būtu "konkrēti, skaidri un leģitīmi", dati netiek turpmāk apstrādāti veidā, kas nav saderīgs ar šiem nolūkiem, un ka apstrādei ir derīgs juridiskais pamats, kā prasīts VDAR 5. pantā. Daži konkrēti piemēri nolūkiem, kādus var norādīt datu pārziņi saistībā ar satīklotajiem transportlīdzekļiem, ir aplūkoti šo pamatnostādņu III daļā, kur arī sniegti konkrēti ieteikumi katram apstrādes veidam.

2.3 Atbilstīgums un datu minimizēšana

70. Lai ievērotu datu minimizēšanas principu[38], transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem un citiem datu pārziņiem būtu jāpievērš īpaša uzmanība to datu kategorijām, kas viņiem nepieciešamas no satīklotā transportlīdzekļa, jo viņi vāc tikai tos personas datus, kas ir būtiski un nepieciešami apstrādei. Piemēram, atrašanās vietas dati it īpaši iejaucas privātajā dzīvē, un tie var atklāt daudzus datu subjektu dzīves paradumus. Attiecīgi nozares dalībniekiem vajadzētu būt īpaši piesardzīgiem un nevākt atrašanās vietas datus, izņemot gadījumus, kad tas ir absolūti nepieciešams apstrādes nolūkā (skatīt apspriedes par atrašanās vietas datiem iepriekš 2.1. iedaļā).

2.4 Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

71. Ņemot vērā satīkloto transportlīdzekļu radīto personas datu apjomu un daudzveidību, EDAK atzīmē, ka datu pārziņiem ir jānodrošina, lai satīkloto transportlīdzekļu kontekstā izvietotās tehnoloģijas būtu konfigurētas tā, lai ievērotu personu privātumu, piemērojot integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma pienākumus, kā prasīts VDAR 25. pantā. Tehnoloģijas būtu jāveido tā, lai pēc iespējas samazinātu personas datu vākšanu, nodrošinātu privātumu aizsargājošos noklusējuma iestatījumus un nodrošinātu, ka datu subjekti ir labi informēti un viņiem ir iespēja viegli mainīt ar viņu personas datiem saistītās konfigurācijas. Īpaši norādījumi par to, kā ražotāji un pakalpojumu sniedzēji var nodrošināt atbilstību integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma prasībām, varētu būt noderīgi nozarei un trešo personu lietotņu nodrošinātājiem.

[38] VDAR 5. panta 1. punkta c) apakšpunkts.

72. Noteikta vispārīga prakse, kas aprakstīta turpmāk, var arī palīdzēt mazināt riskus fiziskām personām attiecībā uz tiesībām un brīvībām, kas saistītas ar satīklotiem transportlīdzekļiem[39].

2.4.1 Vietēja personas datu apstrāde

73. Kopumā transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem un citiem datu pārziņiem, kur vien iespējams, būtu jāizmanto procesi, kas nav saistīti ar personas datiem vai personas datu nosūtīšanu ārpus transportlīdzekļa (t. i., dati tiek apstrādāti iekšēji). Satīkloto transportlīdzekļu raksturs tomēr ietver riskus, piemēram, iespēju, ka ārēji dalībnieki uzbruks vietējai apstrādei, vai vietējo datu noplūdi, pārdodot transportlīdzekļa daļas. Tādēļ būtu jāpievērš pienācīga uzmanība un jāveic drošības pasākumi, lai nodrošinātu, ka vietējā apstrāde ir un paliek vietēja. Šis scenārijs sniedz priekšrocības, garantējot lietotājam vienpersonisku un pilnīgu kontroli pār saviem personas datiem, un tādējādi tas "integrēti" ietver risku saistībā ar datu privātumu, jo īpaši aizliedzot jebkādu datu apstrādi ieinteresētajām personām bez datu subjekta ziņas. Tas arī ļauj apstrādāt sensitīvus datus, piemēram, biometriskos datus vai datus, kas saistīti ar noziedzīgiem nodarījumiem vai citiem pārkāpumiem, kā arī detalizētus atrašanās vietas datus, uz kuriem citādi attiektos stingrāki noteikumi (skatīt turpmāk). Tādā pašā veidā tas ietver mazāk kiberdrošības risku un neietver ilgu gaidīšanas laiku, kas padara to īpaši piemērotu automatizētām braukšanas palīdzības funkcijām. Daži šāda veida risinājumu piemēri varētu būt šādi:

- ekoloģiskas braukšanas lietotnes, kas apstrādā datus transportlīdzeklī, lai iebūvētajā ekrānā reāllaikā sniegtu ekoloģiskas braukšanas padomus;
- lietotnes, kas ietver personas datu nosūtīšanu uz ierīci, piemēram, viedtālruni, kuru lietotājs pilnībā kontrolē (izmantojot, piemēram, *Bluetooth* vai *Wi-Fi*), un kur transportlīdzekļa dati netiek nosūtīti lietotņu nodrošinātājiem vai transportlīdzekļu ražotājiem; tas ietvers, piemēram, viedtālruņu savienošanu, lai izmantotu automobiļa displeju, multimediju sistēmas, mikrofonu (vai citus sensorus) tālruņa zvanu veikšanai utt., ciktāl savāktie dati paliek datu subjekta kontrolē un tiek izmantoti tikai un vienīgi, lai sniegtu pieprasīto pakalpojumu;
- transportlīdzekļa drošību uzlabojošās lietotnes, piemēram, tādas, kas nodrošina stūres rata skaņas signālus vai vibrācijas, ja autovadītājs apdzen automašīnu, nesignalizējot vai pārkāpjot baltās līnijas, vai brīdina par transportlīdzekļa stāvokli (piemēram, brīdinājums par bremžu kluču nodilumu);
- lietotnes noteiktu transportlīdzekļa komandu atbloķēšanai, iedarbināšanai un/vai aktivizēšanai, izmantojot transportlīdzeklī saglabātos autovadītāja biometriskos datus (piemēram, sejas vai balss modeļus vai pirkstu nospiedumu informāciju).

74. Tādas lietotnes kā iepriekš minētās ietver apstrādi, ko fiziska persona veic tikai personisku darbību izpildei (t. i., bez personas datu nosūtīšanas datu pārzinim vai datu apstrādātājam). Tādēļ saskaņā ar VDAR 2. panta 2. punktu **šīs lietotnes neietilpst VDAR piemērošanas jomā.**

75. Tomēr, ja VDAR neattiecas uz personas datu apstrādi, ko fiziska persona veic tikai personiska vai mājsaimnieciska pasākuma gaitā, tā attiecas uz pārziņiem vai apstrādātājiem, kas nodrošina personas datu apstrādes līdzekļus šādām personiska vai mājsaimnieciska rakstura darbībām (automobiļu ražotāji, pakalpojumu sniedzēji utt.) saskaņā ar VDAR 18. apsvērumu. Tādējādi, rīkojoties kā datu pārzinim vai datu apstrādātājam, viņiem jāizstrādā droša lietotne automašīnā un pienācīgi jāievēro integrētas privātuma aizsardzības un privātuma aizsardzības pēc noklusējuma principi. Jebkurā gadījumā saskaņā ar VDAR 78. apsvērumu: "Attīstot, izstrādājot, atlasot un izmantojot lietojumprogrammas, pakalpojumus un preces,

[39] Skatīt arī Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 4/2019 par 25. pantu "Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma", versija 2.0, pieņemtas 2020. gada 20. oktobrī (turpmāk — Pamatnostādnes 4/2019).

kas balstās uz personas datu apstrādi vai apstrādā personas datus savu pienākumu veikšanai, preču, pakalpojumu un lietojumprogrammu ražotāji būtu jāmudina ņemt vērā tiesības uz datu aizsardzību, kad attīsta un izstrādā šādas preces, pakalpojumus un lietojumprogrammas, un pienācīgi ņemt vērā tehnikas līmeni, lai nodrošinātu, ka pārziņi un apstrādātāji spēj izpildīt savus datu aizsardzības pienākumus".[40] No vienas puses, tas veicinās uz lietotājiem orientētu pakalpojumu attīstīšanu, un, no otras puses, tas atvieglos un nodrošinās turpmāku izmantojumu nākotnē, kas varētu atkal ietilpt VDAR piemērošanas jomā. Konkrētāk, EDAK iesaka izstrādāt drošu automašīnas lietotņu platformu, kas fiziski atdalīta no drošībai svarīgām automašīnas funkcijām, lai piekļuve automašīnas datiem nebūtu atkarīga no nevajadzīgām ārējo mākoņu iespējām.

76. Kur vien iespējams, automobiļu ražotājiem un pakalpojumu sniedzējiem būtu jāapsver vietējā datu apstrāde, lai mazinātu mākoņu apstrādes iespējamos riskus, kā tas ir uzsvērts 29. panta darba grupas publicētajā atzinumā par mākoņdatošanu.[41]

77. Kopumā lietotājiem būtu jāspēj kontrolēt, kā viņu dati tiek vākti un apstrādāti transportlīdzeklī:

- informācija par apstrādi jāsniedz valodā, kuru autovadītājs pārvalda (rokasgrāmata, iestatījumi utt.);
- EDAK iesaka pēc noklusējuma apstrādāt tikai tos datus, kas noteikti nepieciešami transportlīdzekļa darbībai. Datu subjektiem vajadzētu būt iespējai aktivizēt vai deaktivizēt datu apstrādi katram atsevišķam nolūkam un pārzinim/apstrādātājam, un viņiem vajadzētu būt iespējai attiecīgos datus dzēst, ņemot vērā datu apstrādes nolūku un juridisko pamatu;
- datus nedrīkst nosūtīt trešām personām (t. i., tikai lietotājiem ir piekļuve datiem);
- dati būtu jāsaglabā tikai tik ilgi, cik tas nepieciešams pakalpojuma sniegšanai vai kā citādi noteikts Savienības vai dalībvalsts tiesību aktos;
- datu subjektiem būtu jāspēj neatgriezeniski izdzēst visus personas datus pirms transportlīdzekļu laišanas pārdošanā;
- datu subjektiem, ja iespējams, vajadzētu būt tiešai piekļuvei šo lietotņu radītajiem datiem.

78. Visbeidzot, kaut arī ne vienmēr ir iespējams izmantot datu vietējo apstrādi katram lietojuma gadījumam, nereti var ieviest "hibrīdo apstrādi". Piemēram, lietošanā balstītas apdrošināšanas kontekstā personas datus par braukšanas stilu (piemēram, spēks, ar kādu tiek iedarbināts bremžu pedālis, nobraukums utt.) var vai nu apstrādāt transportlīdzeklī, vai arī telemātikas pakalpojumu sniedzējs to var apstrādāt apdrošināšanas sabiedrības (datu pārzinis) uzdevumā, lai izveidotu skaitliskus rādītājus, kas apdrošināšanas sabiedrībai tiek nosūtīti noteiktā kārtībā (piemēram, katru mēnesi). Tādā veidā apdrošināšanas sabiedrība neiegūst piekļuvi neapstrādātiem uzvedības datiem, bet tikai kopējam rādītājam, kas ir apstrādes rezultāts. Tas nodrošina, ka integrēti ir ievēroti datu minimizēšanas principi. Tas arī nozīmē, ka lietotājiem jābūt iespējai īstenot savas tiesības, ja datus glabā citas puses: piemēram, saskaņā ar VDAR 17. pantu lietotājam vajadzētu būt iespējai izdzēst datus, kas glabājas automašīnu tehniskās apkopes veikala vai izplatītāja sistēmās.

2.4.2 Anonimizācija un pseidonimizācija

79. Ja ir paredzēta personas datu nosūtīšana ārpus transportlīdzekļa, pirms nosūtīšanas būtu jāapsver iespēja tos anonimizēt. Veicot anonimizāciju, pārzinim būtu jāņem vērā visa

[40] Plašākus ieteikumus par integrēta privātuma aizsardzību un privātuma aizsardzību pēc noklusējuma skatīt arī Pamatnostādnēs 4/2019.

[41] 29. panta darba grupas Atzinums 5/2012 par mākoņdatošanu. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_lv.pdf.

iesaistītā apstrāde, kas potenciāli var izraisīt datu atkārtotu identificēšanu, piemēram, lokāli anonimizētu datu nosūtīšana. EDAK atgādina, ka datu aizsardzības principi nav jāpiemēro anonīmai informācijai, proti, informācijai, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams[42]. Kad datu kopa ir patiesi anonimizēta un personas vairs nav identificējamas, Eiropas datu aizsardzības tiesību aktus vairs nepiemēro. Tā rezultātā anonimizācija attiecīgos gadījumos var būt laba stratēģija, lai saglabātu ieguvumus un mazinātu riskus saistībā ar satīklotiem transportlīdzekļiem.

80. Kā sīki izklāstīts 29. panta darba grupas atzinumā par anonimizācijas metodēm, lai panāktu datu anonimizāciju, var izmantot dažādas metodes, nereti kombinētas.[43]

81. Citas metodes, piemēram, pseidonimizācija[44], var palīdzēt samazināt datu apstrādes radītos riskus, ņemot vērā, ka vairumā gadījumu tieši identificējami dati nav nepieciešami apstrādes nolūka sasniegšanai. Pseidonimizācija, ja to papildina drošības pasākumi, uzlabo personas datu aizsardzību, samazinot ļaunprātīgas izmantošanas risku. Atšķirībā no anonimizācijas pseidonimizācija ir atgriezeniska, un pseidonimizētos datus uzskata par personas datiem, uz kuriem attiecas VDAR.

2.4.3 Novērtējumi par ietekmi uz datu aizsardzību

82. Ņemot vērā to personas datu apjomu un sensitivitāti, ko var ģenerēt, izmantojot satīklotos transportlīdzekļus; ir ticams, ka apstrāde, jo īpaši situācijās, kad personas dati tiek apstrādāti ārpus transportlīdzekļa, bieži radīs augstu risku fizisku personu tiesībām un brīvībām. Šādā gadījumā nozares dalībniekiem būs jāveic novērtējums par ietekmi uz datu aizsardzību (NIDA), lai identificētu un mazinātu riskus, kā sīki aprakstīts VDAR 35. un 36. pantā. Pat gadījumos, kad NIDA nav nepieciešams, to ieteicams veikt pēc iespējas agrāk izstrādes procesā. Tas ļaus nozares dalībniekiem iekļaut šīs analīzes rezultātus dizaina izvēlē pirms jauno tehnoloģiju ieviešanas.

2.5 Informēšana

83. Pirms personas datu apstrādes datu subjektu informē par datu pārziņa identitāti (piemēram, transportlīdzekļa un aprīkojuma ražotājs vai pakalpojumu sniedzējs), apstrādes nolūku, datu saņēmējiem, laikposmu, par kuru dati tiks apstrādāti, kā arī datu subjekta tiesībām saskaņā ar VDAR[45].

84. Turklāt transportlīdzekļa un aprīkojuma ražotājam, pakalpojumu sniedzējam vai citam datu pārzinim būtu arī jāsniedz datu subjektam šāda informācija skaidrā, vienkāršā un viegli pieejamā veidā:

- datu aizsardzības speciālista kontaktinformācija;
- apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats;
- nepārprotama atsauce uz datu pārziņa vai trešās personas īstenotajām leģitīmajām interesēm, ja šādas leģitīmās intereses ir apstrādes juridiskais pamats;
- personas datu saņēmēji vai saņēmēju kategorijas, ja tādas ir;

[42] Skatīt VDAR 4. panta 1. punktu un 26. apsvērumu.
[43] 29. panta datu aizsardzības darba grupa — Atzinums Nr. 05/2014 par anonimizācijas metodēm; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lv.pdf.
[44] VDAR, 4. panta 5. punkts. *Enisa* 2019. gada 3. decembra ziņojums: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] VDAR 5. panta 1. punkta a) apakšpunkts un 13. apsvērums. Skatīt arī 29. panta darba grupas Pamatnostādnes par pārredzamību saskaņā ar Regulu 2016/679 (wp260rev.01) — apstiprinājusi EDAK.

- laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;
- tas, ka pastāv tiesības pieprasīt pārzinim piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu, vai tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību;
- tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot uz piekrišanas pamata veiktas apstrādes likumību pirms šādās atsaukšanas, ja apstrāde ir balstīta uz piekrišanu;
- attiecīgā gadījumā fakts, ka pārzinis plāno nosūtīt personas datus uz trešo valsti vai starptautisku organizāciju, un aizsardzības pasākumi, kas izmantoti to nosūtīšanai;
- informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai datu subjektam ir pienākums personas datus sniegt un kādas sekas var būt gadījumos, kad šādi dati netiek sniegti;
- automatizēta lēmumu pieņemšana, tostarp profilēšana, kas rada juridiskas sekas datu subjektam vai līdzīgi būtiski ietekmē datu subjektu, un nozīmīga informācija par izmantoto loģiku, kā arī šādas apstrādes nozīme un paredzamās sekas datu subjektam. Tas jo īpaši varētu attiekties uz lietošanā balstītas apdrošināšanas pakalpojuma sniegšanu privātpersonām;
- tiesības iesniegt sūdzību uzraudzības iestādei;
- informācija par turpmāko apstrādi;
- kopīgas datu apstrādes gadījumā — skaidra un pilnīga informācija par katra datu pārziņa pienākumiem.

85. Dažos gadījumos personas dati netiek vākti tieši no attiecīgās personas. Piemēram, transportlīdzekļa un aprīkojuma ražotājs var paļauties uz izplatītāju informācijas par transportlīdzekļa īpašnieku apkopošanai, lai sniegtu ārkārtas palīdzības pakalpojumus uz ceļa. Ja dati nav tieši ievākti, transportlīdzekļa un aprīkojuma ražotājs, pakalpojumu sniedzējs vai cits datu pārzinis papildus iepriekš minētajai informācijai norāda arī attiecīgo personas datu kategorijas, avotu, no kura personas dati ir iegūti, un attiecīgā gadījumā, vai šie dati ir iegūti no publiski pieejamiem avotiem. Pārzinim šī informācija jāsniedz saprātīgā termiņā pēc datu iegūšanas un **ne vēlāk kā pirmajā no šādiem datumiem** saskaņā ar VDAR 14. panta 3. punktu: i) mēnesi pēc datu iegūšanas, ņemot vērā konkrētos apstākļus, kādos personas dati tiek apstrādāti, ii) pēc pirmās saziņas ar datu subjektu vai iii) ja šie dati tiek nosūtīti trešai personai, pirms datu nosūtīšanas.

86. Var būt jāsniedz jauna informācija datu subjektiem, ja uz viņiem attiecas jauns datu pārzinis. Palīdzības uz ceļa pakalpojumus, kas mijiedarbojas ar satīklotiem transportlīdzekļiem, var sniegt dažādi datu pārziņi atkarībā no valsts vai reģiona, kurā nepieciešama palīdzība. Jaunajiem datu pārziņiem būtu jāsniedz datu subjektiem nepieciešamā informācija, kad datu subjekti šķērso robežas, un pakalpojumus, kas mijiedarbojas ar satīklotajiem transportlīdzekļiem, nodrošina jauni datu pārziņi.

87. Datu subjektiem adresēto informāciju var sniegt pa līmeņiem[46], t. i., atdalot divus informācijas līmeņus: no vienas puses, pirmā līmeņa informācija, kas ir vissvarīgākā datu subjektiem, un, no otras puses, informācija, kas, domājams, būs aktuāla vēlāk. Būtiskā pirmā līmeņa informācija papildus datu pārziņa identitātei ietver apstrādes nolūku un datu subjekta tiesību aprakstu, kā arī jebkādu papildu informāciju par apstrādi, kas visvairāk skar datu subjektu, un apstrādi, kas viņus varētu pārsteigt. EDAK iesaka saistībā ar satīklotajiem

[46] Skatīt 29. panta darba grupas Pamatnostādnes par pārredzamību saskaņā ar Regulu 2016/679 (wp260rev.01) — apstiprinājusi EDAK.

transportlīdzekļiem datu subjektu informēt par visiem saņēmējiem jau pirmajā informācijas slānī. Kā norādīts 29. panta darba grupas pamatnostādnēs par pārredzamību, pārziņiem būtu jāsniedz informācija par saņēmējiem, kas ir visbūtiskākie datu subjektiem. Praksē parasti tie būs nosauktie saņēmēji, lai datu subjekti precīzi zinātu, kā rīcībā ir viņu personas dati. Ja pārziņi nevar sniegt saņēmēju vārdus, informācijai vajadzētu būt pēc iespējas precīzākai, norādot saņēmēja veidu (t. i., atsaucoties uz tā veiktajām darbībām), nozari, sektoru un apakšsektoru, kā arī saņēmēju atrašanās vietu.

88. Datu subjektus var informēt, izmantojot kodolīgus un viegli saprotamus noteikumus transportlīdzekļa pārdošanas līgumā, pakalpojumu sniegšanas līgumā un/vai jebkurā rakstiskā veidā, izmantojot atsevišķus dokumentus (piemēram, transportlīdzekļa tehniskās apkopes uzskaites grāmata vai rokasgrāmata) vai iebūvēto datoru.

89. Papildus vajadzīgajai informācijai var izmantot standartizētas ikonas, kā prasīts VDAR 13. un 14. pantā, lai uzlabotu pārredzamību, potenciāli samazinot nepieciešamību iesniegt datu subjektam liela apjoma rakstisku informāciju. Tam vajadzētu būt redzamam transportlīdzekļos, lai saistībā ar plānoto apstrādi sniegtu labu pārskatu saprotamā un skaidri salasāmā veidā. EDAK uzsver šo ikonu standartizācijas nozīmi, lai lietotājs redzētu vienus un tos pašus simbolus neatkarīgi no transportlīdzekļa markas vai modeļa. Piemēram, ja tiek apkopoti noteikta veida dati, tādi kā atrašanās vieta, transportlīdzekļu bortā varētu parādīties skaidrs signāls (piemēram, gaisma transportlīdzekļa iekšpusē), lai informētu pasažierus par datu vākšanu.

2.6 Datu subjekta tiesības

90. Transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem un citiem datu pārziņiem būtu jāsekmē datu subjektu kontrole pār viņu datiem visā apstrādes laikposmā, ieviešot īpašus rīkus, kas nodrošina efektīvu veidu savu tiesību īstenošanai, jo īpaši tiesības piekļūt datiem, labot un dzēst datus, tiesības ierobežot apstrādi un — atkarībā no apstrādes juridiskā pamata — tiesības uz datu pārnesamību un tiesības iebilst pret apstrādi.

91. Lai atvieglotu iestatījumu modifikācijas, būtu jāievieš profila pārvaldības sistēma, kas saglabātu zināmo autovadītāju izvēles un palīdzētu viņiem jebkurā laikā viegli mainīt savus privātuma iestatījumus. Profila pārvaldības sistēmā vajadzētu būt apkopotiem centralizēti visiem datu iestatījumiem katrai datu apstrādei, jo īpaši, lai pēc datu subjekta pieprasījuma atvieglotu piekļuvi personas datiem, to dzēšanu, izņemšanu un pārnešanu no transportlīdzekļu sistēmām. Autovadītājiem vajadzētu būt iespējai jebkurā brīdī uz laiku vai neatgriezeniski pārtraukt noteikta veida datu vākšanu, ja vien nav īpaša juridiska pamata, uz kuru pārzinis var atsaukties, lai turpinātu konkrētu datu vākšanu. Ja runa ir par līgumu, kurā paredzēts personalizēts piedāvājums, pamatojoties uz braukšanas paradumiem, tas var nozīmēt, ka tā rezultātā uz lietotāju attiecas minētā līguma standarta nosacījumi. Šīm funkcijām vajadzētu būt iebūvētām transportlīdzeklī, lai gan tās varētu arī tikt nodrošinātas datu subjektiem, izmantojot papildu līdzekļus (piemēram, īpašu lietotni). Turklāt, lai datu subjekti varētu ātri un viegli izņemt personas datus, kurus var glabāt automašīnas kontrolmērinstrumentu panelī (piemēram, GPS navigācijas vēsture, tīmekļa pārlūkošana utt.), EDAK iesaka ražotājiem nodrošināt vienkāršu funkcionalitāti (piemēram, dzēšanas pogu).

92. Satīklota transportlīdzekļa pārdošanai un no tā izrietošajai īpašumtiesību maiņai vajadzētu arī izdzēst visus personas datus, kas vairs nav vajadzīgi iepriekš norādītajiem nolūkiem, un datu subjektam vajadzētu būt iespējai īstenot savas tiesības uz pārnesamību.

2.7 Drošība

93. Transportlīdzekļu un aprīkojuma ražotājiem, pakalpojumu sniedzējiem un citiem datu pārziņiem būtu jāievieš pasākumi, kas garantē apstrādāto datu drošību un konfidencialitāti,

un jāveic visi lietderīgie piesardzības pasākumi, lai nepieļautu, ka nepilnvarotas personas iegūst kontroli. Nozares dalībniekiem jo īpaši būtu jāapsver šādu pasākumu ieviešana:

- sakaru kanālu šifrēšana, izmantojot jaunākajiem tehnikas sasniegumiem atbilstošu algoritmu;
- šifrēšanas atslēgu pārvaldības sistēmas ieviešana, kas ir unikāla katram transportlīdzeklim, nevis katram modelim;
- glabājot attālināti, datu šifrēšana, izmantojot jaunākajiem tehnikas sasniegumiem atbilstošus algoritmus;
- regulāra šifrēšanas atslēgu atjaunināšana;
- šifrēšanas atslēgu aizsardzība pret jebkādu izpaušanu;
- datu uztveršanas ierīču autentificēšana;
- datu integritātes nodrošināšana (piemēram, izmantojot jaukšanu);
- piemērojot piekļuvei personas datiem uzticamas lietotāju autentifikācijas metodes (parole, elektroniskais sertifikāts utt.);

94. Attiecībā uz jo īpaši transportlīdzekļu ražotājiem EDAK iesaka ieviest šādus drošības pasākumus:

- transportlīdzekļa vitāli svarīgo funkciju nodalīšana no tām, kuras vienmēr ir atkarīgas no telesakaru iespējām (piemēram, "informatīvā izklaide");
- tehnisko pasākumu īstenošana, kas ļauj transportlīdzekļu ražotājiem visā transportlīdzekļa ekspluatācijas laikā ātri novērst drošības nepilnības;
- transportlīdzekļa vitālajām funkcijām pēc iespējas jāpiešķir prioritāte drošu sakaru līdzekļu izmantošanai, kas īpaši paredzēti transportēšanai;
- signalizācijas sistēmas izveidošana, ja tiek uzbrukts transportlīdzekļa sistēmām ar iespēju darboties izlīdzināšanas režīmā[47];
- jebkādas piekļuves transportlīdzekļa informācijas sistēmai reģistrācijas vēsture, piemēram, ne vairāk kā sešus mēnešus iepriekš, lai ļautu saprast jebkura iespējamā uzbrukuma izcelsmi un periodiski veikt reģistrētās informācijas pārskatīšanu nolūkā konstatēt iespējamās anomālijas.

95. Šie vispārīgie ieteikumi būtu jāpapildina ar konkrētām prasībām, ņemot vērā katras datu apstrādes īpatnības un nolūku.

2.8 Personas datu nosūtīšana trešām personām

96. Principā piekļuve satīklota transportlīdzekļa ģenerētiem datiem ir tikai datu pārzinim un datu subjektam. Tomēr datu pārzinis var nosūtīt personas datus komerciālajam partnerim (saņēmējam), ciktāl šāda nosūtīšana likumīgi balstīta kādā no juridiskajiem pamatiem, kas noteikti VDAR 6. pantā.

97. Ņemot vērā transportlīdzekļa lietošanas datu iespējamo sensitivitāti (piemēram, veiktie braucieni, braukšanas stils), EDAK iesaka datu subjekta piekrišanu sistemātiski iegūt pirms datu nosūtīšanas komerciālajam partnerim, kas darbojas kā datu pārzinis (piemēram, atzīmējot lodziņu, kas nav iepriekš atzīmēts, vai, ja tas ir tehniski iespējams, izmantojot fizisku vai loģisku ierīci, kurai persona var piekļūt no transportlīdzekļa). Savukārt

[47] Izlīdzināšanas režīms ir transportlīdzekļa darbības režīms, kas nodrošina, ka tiek garantētas drošai transportlīdzekļa darbībai būtiskas funkcijas (t. i., minimālās drošības prasības), pat ja citas mazāk svarīgas funkcijas tiktu deaktivizētas (piemēram, ģeogrāfiskās vadības ierīces darbību var uzskatīt par nebūtisku atšķirībā no bremžu sistēmas).

komerciālais partneris kļūst atbildīgs par saņemtajiem datiem un uz to attiecas visi VDAR ietvertie noteikumi.

98. Transportlīdzekļa ražotājs, pakalpojumu sniedzējs vai cits datu pārzinis var nosūtīt personas datus datu apstrādātājam, kas piedalās pakalpojumu sniegšanā datu subjektam, ar nosacījumu, ka datu apstrādātājs neizmanto šos datus savām vajadzībām. Datu pārziņi un datu apstrādātāji sagatavo līgumu vai citu juridisku dokumentu, kurā precizē katras puses pienākumus un izklāsta VDAR 28. panta noteikumus.

2.9 Personas datu nosūtīšana ārpus ES/EEZ

99. Ja personas dati tiek nosūtīti ārpus Eiropas Ekonomikas zonas, ir paredzēti īpaši aizsardzības pasākumi, lai nodrošinātu, ka aizsardzība "seko" datiem.

100. Tādējādi datu pārzinis var nosūtīt personas datus saņēmējam tikai tiktāl, ciktāl šāda nosūtīšana atbilst VDAR V nodaļā noteiktajām prasībām.

2.10 Transportlīdzeklī iebūvētu *Wi-Fi* tehnoloģiju izmantošana

101. Mobilo sakaru tehnoloģiju attīstība ļauj ērti izmantot internetu, esot uz ceļa. Kaut arī transportlīdzeklī var nodrošināt *Wi-Fi* savienojamību, izmantojot viedtālruņa tīklāju vai īpašu ierīci (OBD-II sargspraudni, bezvadu modemu vai maršrutētāju utt.), lielākā daļa ražotāju mūsdienās piedāvā modeļus ar iebūvētu mobilo datu savienojumu, kas spēj arī izveidot *Wi-Fi* tīklus. Atkarībā no situācijas jāapsver vairāki aspekti:

- *Wi-Fi* savienojumu kā pakalpojumu piedāvā satiksmes pakalpojumu profesionālis, piemēram, taksometra vadītājs saviem klientiem. Šajā gadījumā profesionāli vai viņa/viņas uzņēmumu var uzskatīt par interneta pakalpojumu sniedzēju (*ISP*), tāpēc uz viņu attiecas īpaši pienākumi un ierobežojumi attiecībā uz viņa/viņas klientu personas datu apstrādi.

- *Wi-Fi* savienojums ir izveidots tikai autovadītāja lietošanai (izņemot autovadītāju un viņa/viņas pasažierus). Šajā gadījumā personas datu apstrāde tiek uzskatīta par tikai personisku vai mājsaimniecisku pasākumu saskaņā ar VDAR 2. panta 2. punkta c) apakšpunktu un 18. apsvērumu.

102. Kopumā interneta savienojuma saskarņu izplatība, izmantojot *Wi-Fi*, rada lielākus riskus fizisku personu privātumam. Patiešām, lietotāji ar savu transportlīdzekļu starpniecību kļūs par nepārtrauktiem raidītājiem, tāpēc tos var identificēt un izsekot. Lai novērstu izsekošanu, transportlīdzekļu un aprīkojuma ražotājiem būtu jāievieš viegli izmantojamas atteikšanās iespējas, nodrošinot, ka borta *Wi-Fi* tīkla pakalpojumu kopas identifikators (*SSID*) netiek vākts.

3 KONKRĒTIE PIEMĒRI

103. Šajā iedaļā aplūkoti pieci konkrēti apstrādes piemēri saistībā ar satīklotiem transportlīdzekļiem atbilstoši scenārijiem, ar kuriem varētu saskarties nozares ieinteresētās personas. Piemēri aptver datu apstrādi, kam nepieciešamas aprēķina spējas, ko nevar lokāli mobilizēt transportlīdzeklī, un/vai personas datu nosūtīšana trešai personai, lai attālināti veiktu turpmāku analīzi vai nodrošinātu papildu funkcionalitāti. Katram apstrādes veidam šajā dokumentā ir norādīti paredzētie nolūki, vākto datu kategorijas, šādu datu glabāšanas termiņš, datu subjektu tiesības, īstenojamie drošības pasākumi un informācijas saņēmēji. Gadījumā, kad kādi no šiem laukiem nav aprakstīti, piemēro iepriekšējā daļā aprakstītos vispārīgos ieteikumus.

104. Izvēlētie piemēri nav izsmeļoši, un tie ilustrē apstrādes veidu dažādību, juridisko pamatu, dalībniekus utt., kas varētu būt saistīti ar satīklotajiem transportlīdzekļiem.

3.1 Pakalpojuma sniegšana ar trešās personas starpniecību

105. Datu subjekti var noslēgt līgumu ar pakalpojumu sniedzēju, lai iegūtu papildvērtības pakalpojumus saistībā ar savu transportlīdzekli. Piemēram, datu subjekts var noslēgt lietošanā balstītu apdrošināšanas līgumu, kas piedāvā samazinātas apdrošināšanas prēmijas, braucot mazāk (“Maksā, kad brauc”), vai par labu braukšanas stilu (apmaksa atbilstoši braukšanas stilam), un tam nepieciešama braukšanas paradumu uzraudzība, ko veic apdrošināšanas sabiedrība. Datu subjekts var arī noslēgt līgumu ar uzņēmumu, kas transportlīdzekļa bojājumu gadījumā piedāvā palīdzību uz ceļa un kas paredz transportlīdzekļa atrašanās vietas informācijas nosūtīšanu uzņēmumam, vai ar pakalpojumu sniedzēju, lai saņemtu ziņojumus vai brīdinājumus par transportlīdzekļa darbību (piemēram, brīdinājums par bremžu nodiluma stāvokli vai atgādinājums par tehniskās apskates datumu).

3.1.1 Lietošanā balstīta apdrošināšana

106. “Maksā, kad brauc” ir lietošanā balstīts apdrošināšanas veids, kas reģistrē autovadītāja veikto nobraukumu un/vai braukšanas paradumus, lai atšķirtu un apbalvotu “drošos”

autovadītājus, piešķirot viņiem mazākas prēmijas. Apdrošinātājs pieprasīs autovadītājam instalēt iebūvētu telemātikas pakalpojumu, mobilo lietotni vai aktivizēt iebūvēto ražotāja moduli, kas reģistrē apdrošināšanas ņēmēja nobraukumu un/vai braukšanas stilu (bremzēšanas modelis, ātrs paātrinājums utt.). Telemātikas ierīces apkopotā informācija tiks izmantota, lai piešķirtu autovadītājam vērtējumu un analizētu, kādus riskus viņš/viņa var radīt apdrošināšanas sabiedrībai.

107. Tā kā lietošanā balstītai apdrošināšanai ir nepieciešama piekrišana saskaņā ar E-privātuma direktīvas 5. panta 3. punktu, EDAK norāda, ka apdrošinājuma ņēmējam ir jābūt izvēlei iegādāties lietošanā nebalstītu apdrošināšanas polisi. Pretējā gadījumā piekrišana netiks uzskatīta par brīvi sniegtu, jo līguma izpilde būtu atkarīga no piekrišanas. Turklāt VDAR 7. panta 3. punktā noteikts, ka datu subjektam jābūt tiesībām atsaukt piekrišanu.

3.1.1.1 Juridiskais pamats

108. Ja datus vāc, izmantojot publiski pieejamu elektronisko sakaru pakalpojumu (piemēram, izmantojot SIM karti, kas atrodas telemātikas ierīcē), lai piekļūtu transportlīdzeklī jau uzglabātajai informācijai, nepieciešama piekrišana, kā paredzēts E-privātuma direktīvas 5. panta 3. punktā. Nevienu no minētajos noteikumos paredzētajiem atbrīvojumiem šajā gadījumā nevar piemērot: apstrāde nav paredzēta vienīgi, lai veiktu saziņas pārraidīšanu elektronisko sakaru tīklā, un tā neattiecas arī uz informācijas sabiedrības pakalpojumu, kuru skaidri pieprasījis abonents vai lietotājs. Piekrišanu bija iespējams iegūt līguma noslēgšanas brīdī.

109. Attiecībā uz personas datu apstrādi pēc datu uzglabāšanas vai piekļuves galalietotāja galiekārtai, apdrošināšanas sabiedrība šajā konkrētajā kontekstā var atsaukties uz VDAR 6. panta 1. punkta b) apakšpunktu, ja vien tā var konstatēt, ka apstrāde tiek veikta spēkā esoša līguma ar datu subjektu ietvaros un šī apstrāde ir nepieciešama, lai varētu izpildīt konkrēto līgumu ar datu subjektu. Ciktāl apstrāde ir objektīvi nepieciešama līguma izpildei ar datu subjektu, EDAK uzskata, ka, atsaucoties uz VDAR 6. panta 1. punkta b) apakšpunktu, šajā konkrētajā gadījumā netiktu mazināta E-privātuma direktīvas 5. panta 3. punktā paredzētā papildu aizsardzība. Šis juridiskais pamats tiek realizēts, datu subjektam parakstot līgumu ar apdrošināšanas sabiedrību.

3.1.1.2 Savāktie dati

110. Jāņem vērā divu veidu personas dati:

- **komerciālie un darījumu dati:** datu subjekta identifikācijas informācija, ar darījumiem saistīti dati, dati par maksāšanas līdzekļiem utt.;
- **lietošanas dati:** personas dati, ko ģenerē transportlīdzeklis, braukšanas paradumi, atrašanās vieta utt.

111. EDAK iesaka, ciktāl iespējams, un ņemot vērā risku, ka ar telemātikas lodziņa palīdzību savāktos datus var izmantot neatļauti, lai izveidotu precīzu autovadītāja kustību profilu, neapstrādāti dati par braukšanas stilu būtu vai nu jāapstrādā:

- transportlīdzekļa iekšienē telemātikas lodziņos vai lietotāja viedtālrunī, lai apdrošinātājs piekļūtu tikai rezultātu datiem (piemēram, vērtējumam, kas saistīts ar braukšanas paradumiem), nevis detalizētiem neapstrādātiem datiem (skatīt 2.1. iedaļu);
- vai telemātikas pakalpojumu sniedzējam pārziņa uzdevumā (apdrošināšanas sabiedrība), lai izveidotu skaitlisku vērtējumu, kas tiek nodots apdrošināšanas sabiedrībai saskaņā ar noteiktu pamatu. Šajā gadījumā ir jānodala neapstrādāti dati un dati, kas tieši attiecas uz autovadītāja identitāti. Tas nozīmē, ka telemātikas pakalpojumu sniedzējs saņem reāllaika datus, bet nezina apdrošināšanas ņēmēju vārdus, automašīnu valsts reģistrācijas numurus utt. Savukārt apdrošinātājs zina apdrošināšanas ņēmēju vārdus, bet saņem tikai vērtējumu un kopējos kilometrus, nevis izejas datus, kas izmantoti šādu vērtējumu iegūšanai.

112. Turklāt jāatzīmē, ka, ja līguma izpildei ir nepieciešams tikai nobraukums, atrašanās vietas datus nedrīkst vākt.

3.1.1.3 Glabāšanas termiņš

113. Saistībā ar datu apstrādi, ko veic, lai izpildītu līgumu (t. i., pakalpojuma sniegšanu), pirms noteikt to attiecīgos glabāšanas termiņus, ir svarīgi nošķirt divu veidu datus:

- **komerciālie un darījumu dati:** šos datus var glabāt aktīvā datu bāzē visu līguma darbības laiku. Līguma beigās tos var fiziski (uz atsevišķa datu nesēja: DVD utt.) vai loģiski (autorizācijas pārvaldībā) arhivēt iespējamu tiesvedību nolūkiem. Pēc tam likumā paredzētā noilguma termiņa beigās datus dzēš vai anonimizē;

- **lietošanas dati:** lietošanas datus var klasificēt kā neapstrādātus datus un kā apkopotus datus. Kā minēts iepriekš, datu pārziņiem vai apstrādātājiem, ja iespējams, nevajadzētu apstrādāt neapstrādātus datus. Ja tas ir nepieciešams, neapstrādāti dati būtu jāglabā tikai tik ilgi, kamēr tie ir vajadzīgi apkopoto datu izstrādei un minētā apkopošanas procesa derīguma pārbaudei. Apkopotie dati būtu jāsaglabā tikai tik ilgi, cik tas nepieciešams pakalpojuma sniegšanai vai kā citādi pieprasīts Savienības vai dalībvalsts tiesībās.

3.1.1.4 Datu subjektu informēšana un tiesības

114. Saskaņā ar VDAR 13. pantu pirms personas datu apstrādes datu subjektu par to informē pārredzamā un saprotamā veidā. Jo īpaši viņš/viņa jāinformē par laikposmu, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai. Šajā pēdējā gadījumā EDAK iesaka izmantot pedagoģisku pieeju, lai uzsvērtu atšķirību starp neapstrādātiem datiem un uz šī pamata iegūto vērtējumu, uzsverot, ka šādā gadījumā apdrošinātājs apkopos rādītāja rezultātu tikai vajadzības gadījumā.

115. Ja datus neapstrādā transportlīdzeklī, bet pārziņa (apdrošināšanas sabiedrības) uzdevumā apstrādi veic telemātikas pakalpojumu sniedzējs, informācijā būtu lietderīgi minēt, ka šajā gadījumā pakalpojumu sniedzējam nebūs piekļuves datiem, kas tieši saistīti ar autovadītāja personas identitāti (piemēram, vārdi, reģistrācijas numura zīmes utt.). Ņemot vērā arī to, ka ir svarīgi informēt datu subjektus par viņu personas datu apstrādes sekām un to, ka viņu datu apstrāde datu subjektiem nedrīkst būt pārsteigums, EDAK iesaka datu subjektu informēt par profilēšanas esību un šādas profilēšanas sekām, pat ja tas neietver automatizētu lēmumu pieņemšanu, kā minēts VDAR 22. pantā.

116. Attiecībā uz datu subjektu tiesībām viņus īpaši informē par pieejamajiem līdzekļiem savu piekļuves, labošanas, apstrādes ierobežošanas un datu dzēšanas pieprasīšanas tiesību īstenošanai. Tā kā šajā kontekstā vāktos neapstrādātos datus sniedz datu subjekts (izmantojot īpašas veidlapas vai ar savu rīcību) un tos apstrādā, pamatojoties uz VDAR 6. panta 1. punkta b) apakšpunktu (līguma izpilde), datu subjekts var īstenot savas tiesības uz datu pārnesamību. Kā uzsvērts pamatnostādnēs par tiesībām uz datu pārnesamību, EDAK stingri iesaka "datu pārziņiem nepārprotami izskaidrot atšķirību starp tādu datu veidiem, kurus datu subjekts var saņemt, izmantojot subjekta piekļuves tiesības un tiesības uz datu pārnesamību".[48]

117. Informāciju var sniegt, kad ir parakstīts līgums.

3.1.1.5 Saņēmējs:

118. EDAK iesaka transportlīdzekļa lietošanas datus, cik vien iespējams, apstrādāt tieši telemātikas lodziņos, lai apdrošinātājs piekļūtu tikai rezultātu datiem (piemēram, vērtējumam), nevis detalizētiem neapstrādātiem datiem.

[48] 29. panta darba grupa, Pamatnostādnes par tiesībām uz datu pārnesamību saskaņā ar Regulu 2016/676, WP242 rev.01, apstiprinājusi EDAK, 13. lpp.

119. Ja telemātikas pakalpojumu sniedzējs datus vāc pārziņa (apdrošināšanas sabiedrības) uzdevumā, lai iegūtu skaitlisku vērtējumu, tam nav jāzina apdrošināšanas ņēmēju autovadītāja identitāte (piemēram, vārdi, reģistrācijas numura zīmes utt.).

3.1.1.6 Drošība:

120. Piemēro vispārīgos ieteikumus. Skatīt 2.7. iedaļu.

3.1.2 Autostāvvietas noma un rezervēšana

121. Autostāvvietas īpašnieks var vēlēties to iznomāt. Šim nolūkam viņš/viņa ievieto sludinājumu un nosaka tās cenu tīmekļa lietotnē. Pēc tam, kad autostāvvietas nomas sludinājums ir ievietos, lietotne informē īpašnieku, kad autovadītājs vēlas to rezervēt. Autovadītājs var izvēlēties galamērķi un pārbaudīt pieejamās autostāvvietas, pamatojoties uz vairākiem kritērijiem. Pēc īpašnieka apstiprinājuma darījums tiek apstiprināts, un pakalpojumu sniedzējs apstrādā maksājuma transakciju, pēc tam ar navigācijas palīdzību sniedz norādes uz atrašanās vietu.

3.1.2.1 Juridiskais pamats

122. Ja dati tiek vākti, izmantojot publiski pieejamu elektronisko saziņu, piemēro E-privātuma direktīvas 5. panta 3. punktu.

123. Tā kā šis ir informācijas sabiedrības pakalpojums, E-privātuma direktīvas 5. panta 3. punkts neprasa iegūt piekrišanu, lai piekļūtu transportlīdzeklī jau uzglabātai informācijai, ja abonents nepārprotami pieprasa šādu pakalpojumu.

124. Personas datu apstrādei un tikai datiem, kas vajadzīgi līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei, juridiskais pamats būs VDAR 6. panta 1. punkta b) apakšpunkts.

3.1.2.2 Savāktie dati

125. Apstrādātie dati ietver autovadītāja kontaktinformāciju (vārds, e-pasts, tālruņa numurs, transportlīdzekļa tips (piemēram, vieglā automašīna, kravas automašīna, motocikls), reģistrācijas numura zīmes numuru, stāvēšanas periodu, maksājuma informāciju (piemēram, kredītkartes informāciju), kā arī navigācijas datus.

3.1.2.3 Glabāšanas termiņš

126. Dati būtu jāglabā tikai tik ilgi, kamēr tas ir nepieciešams stāvvietas līguma izpildei vai citādi, kā paredzēts Savienības vai dalībvalsts tiesību aktos. Pēc tam dati tiek anonimizēti vai dzēsti.

3.1.2.4 Datu subjektu informēšana un tiesības

127. Saskaņā ar VDAR 13. pantu pirms personas datu apstrādes datu subjektu būtu jāinformē pārredzamā un saprotamā veidā .

128. Datu subjektu jo īpaši būtu jāinformē par pieejamajiem līdzekļiem savu piekļuves, labošanas, apstrādes ierobežošanas un datu dzēšanas pieprasīšanas tiesību īstenošanai. Tā kā šajā kontekstā vāktos neapstrādātos datus sniedz datu subjekts (izmantojot īpašas veidlapas vai ar savu rīcību) un tos apstrādā, pamatojoties uz VDAR 6. panta 1. punkta b) apakšpunktu (līguma izpilde), datu subjekts var īstenot savas tiesības uz datu pārnesamību. Kā uzsvērts pamatnostādnēs par tiesībām uz datu pārnesamību, EDAK stingri iesaka "*datu pārziņiem nepārprotami izskaidrot atšķirību starp tādu datu veidiem, kurus datu subjekts var saņemt, izmantojot subjekta piekļuves tiesības un tiesības uz datu* pārnesamību".

3.1.2.5 Saņēmējs:

129. Principā piekļuve datiem ir tikai datu pārzinim un datu apstrādātājam.

3.1.2.6 Drošība:

130. Piemēro vispārīgos ieteikumus. Skatīt 2.7. iedaļu.

3.2 *eZvans*

131. Nopietnas avārijas gadījumā Eiropas Savienībā transportlīdzeklis automātiski iedarbina *eZvanu* uz numuru "112", kas ir ES mēroga avārijas dienestu izsaukšanas numurs (sīkāku informāciju skatīt 1.1. iedaļā), kas ļauj nekavējoties nosūtīt ātrās palīdzības automašīnu uz negadījuma vietu saskaņā ar 2015. gada 29. aprīļa Regulu (ES) 2015/758 par tipa apstiprinājuma prasībām transportlīdzekļa *eZvana* sistēmas izveidošanai uz pakalpojuma "112" bāzes un ar ko groza Direktīvu 2007/46/EK (turpmāk — Regula (ES) 2015/758).

132. Patiešām, transportlīdzekļa iekšpusē uzstādītais *eZvana* ģenerators, kas ļauj pārraidīt caur publisko mobilo bezvadu sakaru tīklu, veic ārkārtas izsaukumu vai nu automātiski, aktivējoties transportlīdzekļa sensoriem, vai arī manuāli, transportlīdzekļa pasažieriem veicot eZvanu tikai gadījumā, ja noticis negadījums. Papildus balss savienojuma aktivizēšanai otrais notikums, kas automātiski aktivizējas negadījuma rezultātā, ir minimālā datu kopuma (MDK) ģenerēšana un nosūtīšana uz ārkārtas izsaukumu centrāli (ĀIC).

3.2.1 Juridiskais pamats

133. Attiecībā uz E-privātuma direktīvas piemērošanu jāņem vērā divi noteikumi:

- 9. pants par atrašanās vietas datiem, kas nav informācija par datu plūsmu, un kuri attiecas tikai uz elektronisko sakaru pakalpojumiem;
- 5. panta 3. punkts par piekļuves iegūšanu informācijai, kas glabājas transportlīdzekļa iekšpusē uzstādītajā ģeneratorā.

134. Neskatoties uz to, ka principā šiem noteikumiem ir nepieciešama datu subjekta piekrišana, Regula (ES) 2015/758 ir juridisks pienākums, kas datu pārzinim ir jāpilda (datu subjektam nav reālas vai brīvas izvēles, un viņš nevarēs atteikt viņa/viņas datu apstrādi). Tādējādi Regula (ES) 2015/758 ignorē autovadītāja piekrišanas nepieciešamību attiecībā uz atrašanās vietas datu un MDK apstrādi.[49]

135. Šo datu apstrādes juridiskais pamats būs juridisko pienākumu ievērošana, kā paredzēts VDAR 6. panta 1. punkta c) apakšpunktā (t. i., Regulā (ES) 2015/758).

3.2.2 Savāktie dati

136. Regulā (ES) 2015/578 ir paredzēts, ka datos, ko sūta ar "112" izsaukšanai paredzētu transportlīdzekļa *eZvana* sistēmu, jāietver tikai minimālā informācija, kā minēts standartā EN 15722:2015 "Intelektiskās transporta sistēmas — E-drošība — *eZvana* minimālo datu kopums (MDK)", tostarp šāda informācija:

- norāde, vai *eZvans* aktivizēts manuāli vai automātiski;
- transportlīdzekļa tips;
- transportlīdzekļa identifikācijas numurs (*VIN*);
- transportlīdzekļa spēkiekārtas tips;
- sākotnējā datu ziņojuma ģenerēšanas laika zīmogs šajā *eZvana* incidentā;
- pēdējās zināmās transportlīdzekļa atrašanās vietas platuma un garuma grādi, kas noteikti vēlākajā iespējamajā brīdī pirms ziņojuma ģenerēšanas;
- transportlīdzekļa pēdējais zināmais reālais braukšanas virziens, kas noteikts pēc iespējas vēlāk pirms ziņojuma ģenerēšanas (tikai pēdējās trīs transportlīdzekļa atrašanās vietas).

[49] Jāatzīmē, ka 8-1-f. punkts Padomes sarunu mandātā attiecībā uz priekšlikumu E-privātuma regulai paredz īpašu izņēmumu attiecībā uz *eZvanu*, jo piekrišana nav nepieciešama, ja "ir jānosaka galiekārtas atrašanās vieta, kad lietotājs veic ārkārtas saziņu vai nu uz vienoto Eiropas neatliekamās palīdzības numuru "112", vai uz valsts ārkārtas palīdzības numuru saskaņā ar 13. panta 3. punktu".

3.2.3 Glabāšanas termiņš

137. Regulā (ES) 2015/758 noteikts, ka datus nedrīkst glabāt ilgāk, nekā nepieciešams ārkārtas situāciju apstrādei. Šos datus pilnībā izdzēš, ja tie šim nolūkam vairs nav vajadzīgi. Turklāt *eZvana* sistēmas iekšējā atmiņā datus automātiski un pastāvīgi dzēš. Var uzglabāt tikai datus tikai par trim pēdējām transportlīdzekļa atrāšanās vietām, ja tas ir absolūti nepieciešams pašreizējās atrašanās vietas un kustības virziena noteikšanai atgadījuma laikā.

3.2.4 Datu subjektu informēšana un tiesības

138. Regulas (ES) 2015/758 6. pantā noteikts, ka ražotāji sniedz skaidru un pilnīgu informāciju par datu apstrādi, izmantojot *eZvana* sistēmu. Šī informācija pirms sistēmas lietošanas tiek sniegta īpašnieka rokasgrāmatā atsevišķi par "112" izsaukšanai paredzēto transportlīdzekļa eZvana sistēmu" un visām trešo personu atbalstītajām *eZvanu* sistēmām. Iekļauta šāda informācija:

- atsauce uz juridisko pamatu apstrādei;
- fakts, ka "112" izsaukšanai paredzētā transportlīdzekļa *eZvana* sistēma tiek aktivēta pēc noklusējuma;
- tādas datu apstrādes mehānismi, ko veic "112" izsaukšanai paredzētā transportlīdzekļa *eZvana* sistēma;
- *eZvana* apstrādes konkrētais nolūks, kas var būt tikai Regulas (ES) 2015/758 5. panta 2. punkta pirmajā daļā minētās ārkārtas situācijas;
- savākto un apstrādāto datu veidi un šo datu saņēmēji;
- datu glabāšanas ilgums "112" izsaukšanai paredzētajā transportlīdzekļa *eZvana* sistēmā;
- fakts, ka netiek veikta transportlīdzekļa pastāvīga uzraudzība;
- datu subjekta tiesību īstenošanas mehānismi, kā arī kontaktdienests, kas ir atbildīgs par piekļuves pieprasījumu apstrādi;
- jebkura nepieciešamā papildu informācija par izsekojamību, uzraudzību un personas datu apstrādi saistībā ar trešās personas pakalpojuma (TPP) *eZvana* un/vai citu papildvērtības pakalpojumu sniegšanu, par ko jāsaņem skaidri izteikta īpašnieka piekrišana un kas atbilst VDAR. Īpaši jāņem vērā fakts, ka var pastāvēt atšķirības datu apstrādē, to veicot ar "112" izsaukšanai paredzēto transportlīdzekļa *eZvana* sistēmu un TPP transportlīdzekļa *ezvana* sistēmu vai citiem papildvērtības pakalpojumiem.

139. Turklāt pakalpojumu sniedzējs pārredzamā un saprotamā veidā sniedz arī datu subjektiem informāciju atbilstīgi VDAR 13. pantam. Jo īpaši viņš vai viņa ir jāinformē par apstrādes nolūkiem, kādiem paredzēts izmantot personas datus, kā arī par to, ka personas datu apstrādes pamatā ir juridisks pienākums, kas pārzinim ir jāpilda.

140. Turklāt, ņemot vērā apstrādes raksturu, informācijai par personas datu saņēmējiem vai saņēmēju kategorijām vajadzētu būt skaidrai un datu subjekti būtu jāinformē, ka dati nav pieejami nevienai struktūrai ārpus "112" izsaukšanai paredzētās transportlīdzekļa *eZvana* sistēmas pirms *eZvana* aktivizēšanas.

141. Attiecībā uz datu subjektu tiesībām jāatzīmē, ka, tā kā apstrādes pamatā ir juridisks pienākums, tiesības iebilst un tiesības uz pārnesamību nav attiecināmas.

3.2.5 Saņēmējs:

142. Pirms nav aktivēts *eZvana* izsaukums, šie dati ārpus "112" izsaukšanai paredzētās transportlīdzekļa *eZvana* sistēmas nav pieejami nevienai struktūrai.

143. Kad to aktivizē (vai nu manuāli transportlīdzeklī sēdošās personas, vai automātiski, tiklīdz transportlīdzekļa sensors konstatē nopietnu sadursmi), *eZvana* sistēma izveido balss savienojumu ar attiecīgo ĀIC, un MDK tiek nosūtīts ĀIC operatoram.

144. Turklāt ar "112" izsaukšanai paredzētās transportlīdzekļa sistēmas *eZvana* starpniecību nosūtītos un ĀIC apstrādātos datus neatliekamās palīdzības dienestam un saistītiem pakalpojumu sniedzējiem, kas minēti Lēmumā Nr. 585/2014/ES, var pārsūtīt tikai ar *eZvana* izsaukumiem saistītu incidentu gadījumā un ar nosacījumiem, kas izklāstīti minētajā lēmumā, un tos var izmantot tikai minētā lēmuma mērķu sasniegšanai. Datus, ko apstrādājuši ĀIC, izmantojot "112" izsaukšanai paredzēto transportlīdzekļa *eZvana* sistēmu, bez datu subjekta skaidras iepriekšējas piekrišanas nevienai trešai personai nenosūta.

3.2.6 Drošība

145. Regula (ES) 2015/758 nosaka prasības *eZvana* sistēmā iekļaut tehnoloģijas, kas pastiprina privātās dzīves neaizskaramību, lai lietotājiem piedāvātu atbilstošu privātuma aizsardzības līmeni, kā arī nepieciešamās garantijas, lai novērstu novērošanu un ļaunprātīgu izmantošanu. Turklāt ražotājiem būtu jānodrošina, ka "112" izsaukšanai paredzētā *eZvana* sistēma, kā arī jebkura cita sistēma, kas nodrošina *eZvanu*, kuru apstrādā trešo personu pakalpojumu sniedzēji vai papildvērtības pakalpojumu sniedzēji, ir izveidota tā, lai nebūtu iespējama personas datu apmaiņa starp šīm sistēmām.

146. Attiecībā uz ĀIC dalībvalstīm būtu jānodrošina personas datu aizsardzība pret ļaunprātīgu izmantošanu, tostarp nelikumīgu piekļuvi, sagrozīšanu vai pazaudēšanu, un tas, lai personas datu glabāšanas, glabāšanas ilguma, apstrādes un aizsardzības protokoli tiktu noteikti vajadzīgajā līmenī un pienācīgi ievēroti.

3.3 Negadījumu izpēte

147. Datu subjekti var brīvprātīgi piekrist piedalīties negadījumu izpētē, kuras mērķis ir labāk izprast ceļu satiksmes negadījumu cēloņus un vispārīgāki zinātniski mērķi.

3.3.1 Juridiskais pamats

148. Ja dati tiek vākti, izmantojot publisku elektronisko sakaru pakalpojumu, datu pārzinim jāsaņem datu subjekta piekrišana, lai iegūtu piekļuvi transportlīdzeklī jau uzglabātajai informācijai, kā paredzēts E-privātuma direktīvas 5. panta 3. punktā. Nevienu no minētajos noteikumos paredzētajiem atbrīvojumiem šajā gadījumā nevar piemērot: apstrāde nav paredzēta tikai nolūkā veikt sakaru pārraidi elektronisko sakaru tīklā, un tā neattiecas arī uz informācijas sabiedrības pakalpojumu, kuru nepārprotami pieprasījis abonents vai lietotājs.

149. Attiecībā uz personas datu apstrādi un ņemot vērā negadījumu izpētei nepieciešamo personas datu daudzveidību un apjomu, EDAK iesaka apstrādi balstīt datu subjekta iepriekšējā piekrišanā saskaņā ar VDAR 6. pantu. Šāda iepriekšēja piekrišana ir jāsniedz uz īpašas veidlapas, ar kuras palīdzību datu subjekts brīvprātīgi piedalās pētījumā un piekrīt, ka šim nolūkam tiek apstrādāti viņa/viņas personas dati. Piekrišana ir tās personas brīvas, konkrētas un apzinātas gribas izpausme, kuras dati tiek apstrādāti (piemēram, atzīmējot lodziņu, kas nav iepriekš atzīmēts, vai konfigurējot iebūvēto datoru, lai aktivizētu funkciju transportlīdzeklī). Šāda piekrišana ir jāsniedz atsevišķi, konkrētiem nolūkiem, un to nevar apkopot vienā produktā ar jauna automobiļa pirkuma vai līzinga līgumu, un turklāt piekrišanas atsaukšanai ir jābūt tikpat vienkāršai kā sniegšanai. Piekrišanas atsaukšanas rezultātā apstrāde tiek pārtraukta. Pēc tam datus dzēš no aktīvās datu bāzes vai tos anonimizē.

150. Piekrišanu, kas ir paredzēta E-privātuma direktīvas 5. panta 3. punktā, un piekrišanu, kas nepieciešama kā juridisks pamats datu apstrādei, var iegūt vienlaikus (piemēram, atzīmējot lodziņu, kurā skaidri norādīts, kam datu subjekts piekrīt).

151. Jāatzīmē, ka atkarībā no apstrādes nosacījumiem (datu pārziņa veida utt.) ir iespējams likumīgi izvēlēties citu juridisko pamatu, ja vien tas nesamazina E-privātuma direktīvas 5. panta 3. punktā paredzēto papildu aizsardzību (skatīt 15. punktu). Ja apstrāde ir balstīta citā juridiskajā pamatā, piemēram, lai izpildītu uzdevumu, ko veic sabiedrības interesēs (VDAR 6. panta 1. punkta e) apakšpunkts), EDAK iesaka datu subjektus iekļaut pētījumā pēc brīvprātības principa.

3.3.2 Savāktie dati

152. Datu pārzinis vāc tikai tos personas datus, kas ir noteikti nepieciešami apstrādei.

153. Jāņem vērā divu veidu dati:

- **dati par dalībniekiem un transportlīdzekļiem;**
- **transportlīdzekļu tehniskie dati** (momentānais ātrums utt.).

154. Zinātniskie pētījumi, kas saistīti ar negadījumiem, pamato momentānā ātruma vākšanu, tostarp ko veic juridiskas personas, kuras tiešā nozīmē neadministrē sabiedriskos pakalpojumus.

155. Patiešām, kā minēts iepriekš, EDAK uzskata, ka negadījumu izpētes kontekstā vāktais momentānais ātrums nav dati, kas saistīti ar noziedzīgiem nodarījumiem pēc būtības (t. i., tie netiek vākti, lai izmeklētu nodarījumu vai sauktu pie atbildības par pārkāpumu), tāpēc ir pamatota to vākšana, ko veic juridiskas personas, kuras tiešā nozīmē neadministrē sabiedriskos pakalpojumus.

3.3.3 Glabāšanas termiņš

156. Ir svarīgi nošķirt divu veidu datus. Pirmkārt, datus par dalībniekiem un transportlīdzekļiem var glabāt visa pētījuma laikā. Otrkārt, transportlīdzekļu tehniskie dati šim nolūkam būtu jāglabā pēc iespējas īsāku laikposmu. Šajā sakarā pieci gadi no pētījuma beigu datuma šķiet saprātīgs termiņš. Minētā termiņa beigās datus dzēš vai anonimizē.

3.3.4 Datu subjektu informēšana un tiesības

157. Pirms personas datu apstrādes datu subjektu informē pārredzamā un saprotamā veidā saskaņā ar VDAR 13. pantu. Jo īpaši momentāna ātruma vākšanas gadījumā datu subjekti būtu konkrēti jāinformē par datu vākšanu. Tā kā datu apstrādes pamatā ir piekrišana, datu subjekts ir konkrēti jāinformē par tiesībām jebkurā laikā atsaukt piekrišanu, neskarot piekrišanā balstītas apstrādes likumību, kas veikta pirms tās atsaukšanas. Turklāt, tā kā šajā kontekstā vāktos datus sniedz datu subjekts (izmantojot īpašas veidlapas vai ar savu rīcību) un tos apstrādā, pamatojoties uz VDAR 6. panta 1. punkta a) apakšpunktu (piekrišana), datu subjekts var īstenot savas tiesības uz datu pārnesamību. Kā uzsvērts pamatnostādnēs par tiesībām uz datu pārnesamību, EDAK stingri iesaka "datu pārziņiem nepārprotami izskaidrot atšķirību starp tādu datu veidiem, kurus datu subjekts var saņemt, izmantojot subjekta piekļuves tiesības un tiesības uz datu pārnesamību". Līdz ar to datu pārzinim būtu jānodrošina vienkāršs veids, kā brīvi un jebkurā laikā atsaukt piekrišanu, kā arī jāizstrādā rīki, lai varētu atbildēt uz datu pārnesamības pieprasījumiem.

158. Šo informāciju var sniegt, parakstot veidlapu, ar kuru piekrīt piedalīties negadījumu izpētē.

3.3.5 Saņēmējs

159. Principā piekļuve datiem ir tikai datu pārzinim un datu apstrādātājam.

3.3.6 Drošība

160. Kā minēts iepriekš, ieviestos drošības pasākumus pielāgo datu sensitivitātes līmenim. Piemēram, ja negadījumu izpētes ietvaros tiek vākts momentānais ātrums (vai jebkuri citi dati, kas saistīti ar kriminālsodāmību un noziedzīgiem nodarījumiem), EDAK stingri iesaka ieviest stingrus drošības pasākumus, piemēram:

- pseidonimizācijas pasākumu ieviešana (piemēram, datu slepenās atslēgas jaukšana, piemēram, datu subjekta uzvārds/vārds un sērijas numurs);
- datu, kas attiecas uz momentāno ātrumu un atrašanās vietu, glabāšana atsevišķās datubāzēs (piemēram, izmantojot jaunākajiem tehnikas sasniegumiem atbilstošu šifrēšanas mehānismu ar atšķirīgām atslēgām un apstiprināšanas mehānismiem);
- un/vai atrašanās vietas datu dzēšana, tiklīdz atbilst atsauces notikums vai secība (piemēram, ceļa tips, diena/nakts), un tieši identificējošu datu glabāšana atsevišķā datu bāzē, kurai var piekļūt tikai neliels cilvēku skaits.

3.4 Automašīnu zādzības

161. Datu subjekti zādzības gadījumā var vēlēties mēģināt atrast savu transportlīdzekli, izmantojot atrašanās vietas datus. Atrašanās vietas datu izmantošana atļauta tikai izmeklēšanas vajadzībām un kompetento juridisko iestāžu veikto lietu novērtējumam.

3.4.1 Juridiskais pamats

162. Ja dati tiek vākti, izmantojot publiski pieejamu elektronisko saziņas dienestu, piemēro E-privātuma direktīvas 5. panta 3. punktu.

163. Tā kā šis ir informācijas sabiedrības pakalpojums, E-privātuma direktīvas 5. panta 3. punkts neprasa saņemt piekrišanu, lai piekļūtu transportlīdzeklī jau uzglabātajai informācijai, ja abonents nepārprotami pieprasa šādu pakalpojumu.

164. Attiecībā uz personas datu apstrādi juridiskais pamats atrašanās vietas datu apstrādei būs transportlīdzekļa īpašnieka piekrišana vai attiecīgā gadījumā līguma izpilde (tikai attiecībā uz datiem, kas nepieciešami līguma izpildei, kura līgumslēdzēja puse ir transportlīdzekļa īpašnieks).

165. Piekrišana ir tās personas brīvas, konkrētas un apzinātas gribas izpausme, kuras dati tiek apstrādāti (piemēram, atzīmējot lodziņu, kas nav iepriekš atzīmēts, vai konfigurējot iebūvēto datoru, lai aktivizētu funkciju transportlīdzeklī). Brīvība sniegt piekrišanu ietver iespēju jebkurā laikā atsaukt piekrišanu, par ko datu subjekts būtu skaidri jāinformē. Piekrišanas atsaukšanas rezultātā apstrāde tiek pārtraukta. Pēc tam datus dzēš no aktīvās datu bāzes, anonimizē vai arhivē.

3.4.2 Savāktie dati

166. Atrašanās vietas datus var nosūtīt tikai brīdī, kad tiek paziņots par zādzību, un atlikušajā laikā tos nedrīkst nepārtraukti vākt.

3.4.3 Glabāšanas termiņš

167. Atrašanās vietas datus var glabāt tikai uz laiku, kamēr kompetentās juridiskās iestādes izskata lietu, vai līdz procedūras beigām, lai kliedētu neskaidrības — tas nebeidzas ar transportlīdzekļa zādzības apstiprināšanu.

3.4.4 Datu subjektu informēšana

168. Pirms personas datu apstrādes datu subjektu būtu jāinformē pārredzamā un saprotamā veidā saskaņā ar VDAR 13. pantu. Konkrētāk, EDAK iesaka datu pārzinim uzsvērt, ka netiek veikta pastāvīga transportlīdzekļa izsekošana un atrašanās vietas datus var apkopot un nosūtīt tikai pēc informēšanas par zādzību. Turklāt pārzinim jāsniedz datu subjektam informācija par to, ka datiem piekļūt var tikai pilnvaroti attālinātās novērošanas platformas darbinieki un likumīgi apstiprinātas iestādes.

169. Kas attiecas uz datu subjektu tiesībām, tā kā datu apstrādes pamatā ir piekrišana, datu subjekts būtu konkrēti jāinformē par tiesībām jebkurā laikā atsaukt piekrišanu, neskarot piekrišanā balstītas apstrādes likumību, kas veikta pirms tās atsaukšanas. Turklāt, ja šajā kontekstā vāktos datus sniedz datu subjekti (izmantojot īpašas veidlapas vai ar savu rīcību)

un tos apstrādā, pamatojoties uz VDAR 6. panta 1. punkta a) apakšpunktu (piekrišana) vai 6. panta 1. punkta b) apakšpunktu (līguma izpilde), datu subjekts var īstenot savas tiesības uz datu pārnesamību. Kā uzsvērts pamatnostādnēs par tiesībām uz datu pārnesamību, EDAK stingri iesaka "datu pārziņiem nepārprotami izskaidrot atšķirību starp tādu datu veidiem, kurus datu subjekts var saņemt, izmantojot subjekta piekļuves tiesības un tiesības uz datu pārnesamību".

170. Līdz ar to datu pārzinim būtu jānodrošina vienkāršs veids, kā brīvi un jebkurā laikā atsaukt piekrišanu (tikai gadījumos, kad piekrišana ir juridiskais pamats), kā arī jāizstrādā rīki, lai varētu atbildēt uz datu pārnesamības pieprasījumiem.

171. Informāciju var sniegt, kad ir parakstīts līgums.

3.4.5 Saņēmēji

172. Informējot par zādzību, atrašanās vietas datus var nodot i) pilnvarotiem attālinātās novērošanas platformas darbiniekiem un ii) likumīgi apstiprinātām iestādēm.

3.4.6 Drošība

173. Piemēro vispārīgos ieteikumus. Skatīt 2.7. iedaļu.