Orientările 1/2020 privind prelucrarea datelor cu caracter personal în contextul vehiculelor conectate și al aplicațiilor de mobilitate

Versiunea 2.0

Adoptate la 9 martie 2021

Istoric versiuni

Versiunea 2.0	9 martie 2021	Adoptarea orientărilor în urma consultării publice
Versiunea 1.0	28 ianuarie 2020	Adoptarea orientărilor spre consultare publică

Cuprins

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

ADOPTĂ URMĂTOARELE ORIENTĂRI

1 INTRODUCERE

1. Un simbol al economiei secolului XX, automobilul este unul dintre produsele de larg consum care au avut un impact semnificativ asupra societății în ansamblu. Frecvent asociate cu noțiunea de libertate, automobilele sunt adesea considerate mai mult decât un simplu mijloc de transport. Într-adevăr, acestea reprezintă un spațiu privat în care oamenii se pot bucura de o anumită autonomie de decizie, fără interferențe din exterior. În prezent, pe măsură ce conceptul de vehicule conectate prinde tot mai mult contur, o astfel de viziune nu mai corespunde realității. Conectivitatea la bordul vehiculelor se extinde rapid de la modelele de lux și mărcile premium la modelele produse în serie pentru segmentul mediu al pieței, iar vehiculele devin centre de date uriașe. Nu doar vehiculele, ci și conducătorii auto și pasagerii devin tot mai conectați. De fapt, multe modele lansate pe piață în ultimii ani sunt prevăzute cu senzori integrați și echipamente conectate la bord, care pot colecta și înregistra, printre altele, date privind performanța motorului, stilul de conducere, locurile vizitate și uneori chiar mișcările ochilor conducătorului auto, pulsul acestuia sau date biometrice în scopul identificării unice a unei persoane fizice[2].

2. Acest proces de prelucrare a datelor are loc într-un ecosistem complex, care nu se limitează la actorii tradiționali din industria autovehiculelor, ci este modelat și de apariția unor noi actori din economia digitală. Acești noi actori pot oferi servicii de infotainment, cum ar fi muzică online, informații privind starea drumurilor și traficul, sau pot furniza sisteme și servicii de asistență la conducere, cum ar fi software pentru pilot automat, actualizări ale stării vehiculului, asigurare în funcție de utilizare sau cartografiere dinamică. În plus, întrucât vehiculele sunt conectate prin rețele de comunicații electronice, administratorii infrastructurii rutiere și operatorii de telecomunicații implicați în acest proces joacă, de asemenea, un rol important în ceea ce privește posibilele operațiuni de prelucrare a datelor cu caracter personal ale conducătorilor auto și ale pasagerilor.

3. Vehiculele conectate generează, de asemenea, cantități din ce în ce mai mari de date, multe dintre acestea putând fi considerate date cu caracter personal, deoarece se referă la conducătorii auto sau la pasageri. Chiar dacă datele colectate de un vehicul conectat nu

[1] Referirile la „statele membre” din prezentul document trebuie înțelese ca referiri la „statele membre ale SEE”.
[2] Infograficul „Date și vehiculul conectat” elaborat de Forumul privind viitorul vieții private; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

sunt legate în mod direct de un nume, ci de aspectele și caracteristicile tehnice ale vehiculului, acestea vor viza conducătorul auto sau ocupanții respectivului vehicul. De exemplu, datele referitoare la stilul de conducere sau la distanța parcursă, datele privind uzura pieselor vehiculului, datele de localizare sau datele colectate de camerele de luat vederi se pot referi la comportamentul conducătorului auto, precum și la eventuale alte persoane aflate la bordul vehiculului sau persoane vizate care trec pe lângă acesta. Astfel de date tehnice sunt produse de o persoană fizică și permit identificarea directă sau indirectă a acesteia de către operatorul de date sau de către o altă persoană. Vehiculul poate fi considerat un terminal ce poate fi folosit de utilizatori diferiți. Prin urmare, la fel ca în cazul unui PC, acest posibil număr mare de utilizatori nu afectează caracterul personal al datelor.

4. În 2016, Fédération Internationale de l'Automobile (FIA) a desfășurat o campanie la nivel european intitulată „My Car My Data" (Automobilul meu, datele mele), pentru a afla ce părere au europenii despre vehiculele conectate[3]. Deși a arătat interesul ridicat al conducătorilor auto pentru conectivitate, campania a subliniat, de asemenea, vigilența care trebuie exercitată în ceea ce privește utilizarea datelor generate de vehicule, precum și importanța respectării legislației privind protecția datelor cu caracter personal. Prin urmare, provocarea constă, pentru fiecare parte interesată, în integrarea dimensiunii privind „protecția datelor cu caracter personal" încă din faza de proiectare a produsului și în asigurarea transparenței și a controlului utilizatorilor de vehicule asupra datelor care îi privesc, în conformitate cu considerentul 78 din RGPD. O astfel de abordare contribuie la consolidarea încrederii utilizatorilor și, prin urmare, la dezvoltarea pe termen lung a acestor tehnologii.

1.1 Lucrări conexe

5. Vehiculele conectate au devenit un subiect important pentru autoritățile de reglementare în ultimul deceniu, cu o creștere semnificativă în ultimii ani. Astfel, la nivel național și internațional au fost publicate diverse lucrări cu privire la securitatea și confidențialitatea datelor în contextul vehiculelor conectate. Aceste reglementări și inițiative vizează completarea cadrelor existente privind protecția datelor și confidențialitatea cu norme specifice pentru fiecare sector sau furnizarea de orientări pentru profesioniști.

1.1.1 Inițiative la nivel european și internațional

6. Începând cu 31 martie 2018, instalarea la bordul vehiculului a sistemului eCall bazat pe numărul 112 este obligatorie pentru toate modelele noi de vehicule din categoriile M1 și N1 (autoturisme și vehicule utilitare ușoare)[4][5]. În 2006, Grupul de lucru „Articolul 29" adoptase deja un document de lucru referitor la protecția datelor și la implicațiile asupra vieții private în cadrul inițiativei privind eCall[6]. În plus, după cum s-a discutat anterior, Grupul de lucru „Articolul 29" a adoptat în octombrie 2017 și un aviz privind prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative (STI-C).

7. În ianuarie 2017, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un studiu axat pe securitatea cibernetică și reziliența automobilelor inteligente, care prezintă activele sensibile, precum și amenințările, riscurile aferente, factorii de

[3] Campania „My Car My Data"; http://www.mycarmydata.eu/.
[4] Serviciul eCall interoperabil la nivelul UE; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decizia nr. 585/2014/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind implementarea serviciului eCall interoperabil la nivelul UE. Text cu relevanță pentru SEE; https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32014D0585&from=ro.
[6] Document de lucru referitor la protecția datelor și la implicațiile asupra vieții private în inițiativa eCall; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.

atenuare și posibilele măsuri de securitate care trebuie puse în aplicare[7]. În septembrie 2017, Conferința internațională a comisarilor pentru protecția datelor și a vieții private (ICDPPC) a adoptat o rezoluție privind vehiculele conectate[8]. În fine, în aprilie 2018, Grupul internațional de lucru privind protecția datelor în telecomunicații (IWGDPT) a adoptat, de asemenea, un document de lucru privind vehiculele conectate[9].

1.1.2 Inițiative naționale ale membrilor Comitetului european pentru protecția datelor (CEPD)

8. În ianuarie 2016, Conferința autorităților federale și de stat pentru protecția datelor din Germania și Asociația producătorilor de vehicule din Germania (VDA) au publicat o declarație comună privind principiile referitoare la protecția datelor în contextul vehiculelor conectate și neconectate[10]. În august 2017, Centrul pentru vehicule conectate și autonome (CCAV) din Regatul Unit a publicat un ghid în care sunt enunțate principiile securității cibernetice pentru vehiculele conectate și automatizate, cu scopul de a sensibiliza părțile interesate din sectorul autovehiculelor cu privire la această chestiune[11]. În octombrie 2017, autoritatea franceză pentru protecția datelor, Commission Nationale de l'Informatique et des Libertés (CNIL), a publicat un pachet de măsuri de asigurare a conformității pentru vehiculele conectate, cu scopul de a sprijini părțile interesate în ceea ce privește modul de integrare a protecției datelor începând cu momentul conceperii și în mod implicit, permițând persoanelor vizate să aibă un control eficace asupra datelor lor[12].

1.2 Legislația aplicabilă

9. Cadrul juridic relevant al UE este RGPD. Acesta se aplică în orice situație în care prelucrarea datelor în contextul vehiculelor conectate implică o prelucrare a datelor cu caracter personal ale persoanelor fizice.

10. Pe lângă RGPD, Directiva 2002/58/CE, astfel cum a fost modificată prin Directiva 2009/136/CE (denumită în continuare „Directiva privind viața privată și comunicațiile electronice"), **stabilește un standard specific pentru toți actorii care doresc să stocheze sau să acceseze informații stocate în echipamentul terminal al unui abonat sau utilizator din Spațiul Economic European (SEE).**

11. Într-adevăr, dacă majoritatea dispozițiilor Directivei privind viața privată și comunicațiile electronice (articolul 6, articolul 9 etc.) se aplică doar furnizorilor de servicii publice de comunicații electronice și furnizorilor de rețele de comunicații publice, articolul 5 alineatul (3) din această directivă este o dispoziție generală. Aceasta nu se aplică doar serviciilor de comunicații electronice, ci și oricărei entități, private sau publice, care stochează pe sau citește informații dintr-un echipament terminal, indiferent de natura datelor stocate sau accesate.

---

[7] Securitatea cibernetică și reziliența automobilelor inteligente; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

[8] Rezoluție privind protecția datelor în vehiculele automatizate și conectate; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.

[9] Document de lucru privind vehiculele conectate; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.

[10] Aspecte legate de protecția datelor în cazul utilizării vehiculelor conectate și neconectate; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.

[11] Principiile securității cibernetice pentru vehiculele conectate și automatizate; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.

[12] Pachet de măsuri de asigurare a conformității pentru o utilizare responsabilă a datelor în cadrul vehiculelor conectate; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

12. În ceea ce privește noțiunea de „echipament terminal”, aceasta este definită în Directiva 2008/63/CE[13]. Articolul 1 litera (a) definește echipamentul terminal ca fiind „echipamentul racordat în mod direct sau indirect la interfața unei rețele publice de telecomunicații, în scopul trimiterii, prelucrării sau recepționării de informații; în ambele cazuri de racordare (directă sau indirectă), aceasta se poate efectua prin cablu, fibre optice sau electromagnetic; racordarea este indirectă atunci când echipamentul este amplasat între terminal și interfața rețelei; (b) echipamentul terminal înseamnă de asemenea echipament pentru stațiile de sol pentru comunicații prin satelit”.

13. Prin urmare, sub rezerva îndeplinirii criteriilor menționate mai sus, vehiculul conectat și dispozitivul conectat la acesta ar trebui considerate „echipamente terminale” (precum un computer, un smartphone sau un televizor inteligent) și se aplică dispozițiile articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice, după caz.

14. Astfel cum a subliniat CEPD în Avizul său nr. 5/2019 privind interacțiunea dintre Directiva privind viața privată și comunicațiile electronice și RGPD[14], articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice prevede că, în general, și sub rezerva excepțiilor de la această regulă menționate la punctul 17 de mai jos, este necesar un acord prealabil pentru stocarea de informații sau pentru dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau al unui utilizator. În măsura în care informațiile stocate în echipamentele terminale ale utilizatorilor finali constituie date cu caracter personal, articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice are întâietate asupra articolului 6 din RGPD în ceea ce privește activitatea de stocare sau dobândirea accesului la aceste informații[15]. Pentru a fi legală, orice operațiune de prelucrare a datelor cu caracter personal ulterioară operațiunilor de prelucrare menționate anterior, inclusiv prelucrarea datelor cu caracter personal obținute prin accesarea informațiilor din echipamentul terminal, trebuie să aibă un temei juridic în conformitate cu articolul 6 din RGPD[16].

15. Întrucât operatorul, atunci când solicită acordul pentru stocarea sau accesarea unor informații în temeiul articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice, trebuie să informeze persoana vizată cu privire la toate scopurile prelucrării, inclusiv orice prelucrare ulterioară operațiunilor menționate mai sus („prelucrare ulterioară”), consimțământul în temeiul articolului 6 din RGPD este, în general, temeiul juridic cel mai adecvat pentru prelucrarea datelor cu caracter personal ulterioară unor astfel de operațiuni (în măsura în care persoana vizată își exprimă consimțământul pentru prelucrarea ulterioară în scopul respectiv, a se vedea punctele 53-54 de mai jos). Prin urmare, este probabil ca acest consimțământ să constituie temeiul juridic atât pentru stocarea și accesarea informațiilor deja stocate, cât și pentru prelucrarea ulterioară a datelor cu caracter personal[17]. Într-adevăr, atunci când se evaluează conformitatea cu articolul 6 din RGPD, ar trebui să se țină seama de faptul că

[13] Directiva 2008/63/CE a Comisiei din 20 iunie 2008 privind concurența pe piețele echipamentelor terminale pentru telecomunicații (versiune codificată) (Text cu relevanță pentru SEE); https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX%3A32008L0063.

[14] Comitetul european pentru protecția datelor, Avizul nr. 5/2019 privind interacțiunea dintre Directiva privind viața privată și comunicațiile electronice și RGPD, în special în ceea ce privește competența, sarcinile și prerogativele autorităților pentru protecția datelor, adoptat la 12 martie 2019 (denumit în continuare - „Avizul nr. 5/2019”), punctul 40.

[15] Ibidem, punctul 40.

[16] Ibidem, punctul 41.

[17] Consimțământul prevăzut la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice și cel necesar ca temei juridic pentru prelucrarea datelor (articolul 6 din RGPD) pentru același scop specific pot fi obținute în același timp (de exemplu, prin bifarea unei căsuțe care indică în mod clar pentru ce își exprimă consimțământul persoana vizată).

prelucrarea în ansamblu implică activități specifice pentru care legiuitorul Uniunii a încercat să ofere o protecție suplimentară[18]. În plus, operatorii de date trebuie să țină cont de impactul asupra drepturilor persoanelor vizate atunci când identifică temeiul juridic adecvat, pentru a respecta principiul echității[19]. În concluzie, articolul 6 din RGPD nu poate fi invocat de operatorii de date pentru a reduce protecția suplimentară prevăzută la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.

16. CEPD reamintește faptul că noțiunea de consimțământ din Directiva privind viața privată și comunicațiile electronice este identică cu noțiunea de consimțământ din RGPD și trebuie să îndeplinească toate cerințele în această materie prevăzute la articolul 4 punctul (11) și la articolul 7 din RGPD.

17. Cu toate acestea, deși consimțământul este principiul, articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice prevede o derogare de la cerința exprimării consimțământului în cunoștință de cauză pentru stocarea de informații sau accesarea informațiilor deja stocate în echipamentul terminal în cazul îndeplinirii unuia dintre următoarele criterii:

   - **Derogarea 1:** cu unicul scop de a efectua transmisia comunicației printr-o rețea de comunicații electronice;
   - **Derogarea 2:** în cazul în care acest lucru este strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.

18. În aceste cazuri, prelucrarea datelor cu caracter personal, inclusiv a celor obținute prin accesarea informațiilor din echipamentul terminal, se bazează pe unul dintre temeiurile juridice prevăzute la articolul 6 din RGPD. De exemplu, consimțământul nu este necesar pentru prelucrarea datelor cu caracter personal în scopul furnizării serviciilor de navigație GPS solicitate de persoana vizată, atunci când aceste servicii pot fi considerate drept servicii ale societății informaționale.

1.3 Domeniul de aplicare

19. CEPD ar dori să sublinieze faptul că prezentele orientări au rolul de a facilita respectarea normelor privind prelucrarea legală a datelor cu caracter personal de către o gamă largă de părți interesate care își desfășoară activitatea în acest sector. Totuși, acestea nu sunt menite să acopere toate cazurile de utilizare posibile în acest context sau să ofere îndrumări pentru fiecare situație specifică posibilă.

20. Domeniul de aplicare al prezentului document se axează în special pe prelucrarea datelor cu caracter personal în legătură cu utilizarea în alte scopuri decât cele profesionale a vehiculelor conectate de către persoanele vizate: de exemplu, conducători auto, pasageri, proprietari de vehicule, alți participanți la trafic etc. Mai exact, acesta vizează datele cu caracter personal: (i) prelucrate în interiorul vehiculului, (ii) schimbate între vehicul și dispozitivele personale conectate la acesta (de exemplu, smartphone-ul utilizatorului) sau (iii) colectate local în vehicul și exportate către entități externe (de exemplu, producători de vehicule, administratori de infrastructură, societăți de asigurări, reparatori auto) pentru prelucrare ulterioară.

21. Definiția vehiculului conectat trebuie înțeleasă ca un concept larg în prezentul document. Acesta poate fi definit drept un vehicul echipat cu multe unități electronice de control

[18] Avizul nr. 5/2019, punctul 41.

[19] Comitetul european pentru protecția datelor, Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, Versiunea 2.0, 8 octombrie 2019, punctul 1.

(ECU) conectate prin intermediul unei rețele încorporate la bordul vehiculului, precum și cu facilități de conectivitate care îi permit să facă schimb de informații cu alte dispozitive, atât din interiorul, cât și din exteriorul vehiculului. Ca atare, poate fi realizat schimbul de date între vehicul și dispozitivele personale conectate la acesta, permițând, de exemplu, oglindirea aplicațiilor pentru dispozitive mobile pe unitatea de informații și divertisment a vehiculului. Prezentul document se aplică și aplicațiilor autonome pentru dispozitive mobile, adică independente de vehicul (de exemplu, care se bazează pe utilizarea exclusivă a smartphone-ului), dezvoltate pentru sprijinirea conducătorilor auto, deoarece acestea contribuie la capacitățile de conectivitate ale vehiculului, chiar dacă este posibil ca acestea să nu se bazeze efectiv pe schimbul propriu-zis de date cu vehiculul. Există un număr mare de aplicații variate pentru vehiculele conectate, care pot include[20]:

22. *gestionarea mobilității:* funcții care permit conducătorilor auto să ajungă la destinație rapid și într-un mod eficient din punctul de vedere al costurilor, furnizând informații în timp util cu privire la navigația GPS, condițiile de mediu potențial periculoase (de exemplu, drumuri acoperite de gheață), blocajele în trafic sau drumurile în lucru, asistență legată de parcări sau garaje, optimizarea consumului de combustibil sau taxele de drum;

23. *gestionarea vehiculului:* funcții menite să îi ajute pe conducătorii auto să reducă cheltuielile de funcționare a vehiculului și să asigure o utilizare mai ușoară a acestuia, cum ar fi notificări privind starea vehiculului și atenționări privind lucrările de service, transferul datelor privind utilizarea (de exemplu, pentru serviciile de reparații auto), asigurări personalizate de tip „Pay As/How You Drive” („plătești cât/cum conduci”), operațiuni la distanță (de exemplu, pornirea sistemului de încălzire) sau memorarea unor setări (de exemplu, poziția scaunului);

24. *siguranța rutieră:* funcții care avertizează conducătorul auto cu privire la pericolele externe și răspunsurile interne, cum ar fi protecția în caz de coliziune, avertizări de pericol, avertizări la depășirea involuntară a benzii de circulație, detectarea stării de somnolență a șoferului, apel de urgență (eCall) sau „cutii negre” pentru investigarea accidentelor (dispozitive de înregistrare a datelor privind evenimentele);

25. *divertisment:* funcții care furnizează informații și asigură divertismentul conducătorului auto și al pasagerilor, cum ar fi interfețe pentru smartphone (apeluri telefonice utilizând funcția „mâini-libere”, mesaje vocale), puncte de acces WLAN, muzică, videoclipuri, internet, platforme de comunicare socială, servicii de tip birou mobil sau „casă inteligentă”;

26. *asistență pentru conducătorul auto:* funcții care implică conducerea parțial sau complet automatizată, cum ar fi asistență operațională sau pilot automat în trafic aglomerat, în parcare sau pe autostradă;

27. *bunăstare:* funcții care monitorizează starea de confort și capacitatea șoferului de a conduce vehiculul, cum ar fi detectarea stării de oboseală sau asistență medicală.

28. Prin urmare, vehiculele pot fi conectate sau nu în mod nativ, iar datele cu caracter personal pot fi colectate prin mai multe mijloace, inclusiv: (i) senzori montați pe vehicul, (ii) dispozitive telematice sau (iii) aplicații pentru dispozitive mobile (de exemplu, accesate de pe un dispozitiv care aparține conducătorului auto). Pentru a face obiectul prezentului document, aplicațiile pentru dispozitive mobile trebuie să fie legate de conducerea vehiculului. De exemplu, aplicațiile de navigație GPS intră sub incidența prezentului

[20] PwC Strategy 2014. „In the fast lane. The bright future of connected cars” („Pe banda rapidă: viitorul strălucit al vehiculelor conectate”): https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

document. În schimb, aplicațiile care doar sugerează conducătorilor auto anumite puncte de interes (restaurante, monumente istorice etc.) nu fac obiectul prezentelor orientări.

29. O mare parte dintre datele generate de un vehicul conectat se referă la o persoană fizică identificată sau identificabilă și, prin urmare, constituie date cu caracter personal. Acestea includ, de exemplu, date identificabile în mod direct (cum ar fi identitatea completă a conducătorului auto), precum și în mod indirect, cum ar fi detalii privind călătoriile efectuate, datele privind utilizarea vehiculului (de exemplu, date referitoare la stilul de conducere sau distanța parcursă) sau datele tehnice ale vehiculului (de exemplu, date referitoare la uzura pieselor vehiculului), care, prin trimiteri la alte fișiere și în special la numărul de identificare al vehiculului (VIN), pot fi asociate cu o persoană fizică. Datele cu caracter personal din vehiculele conectate pot include, de asemenea, metadate, cum ar fi starea de întreținere a vehiculului. Cu alte cuvinte, orice date care pot fi asociate cu o persoană fizică intră sub incidența prezentului document.

30. Ecosistemul vehiculelor conectate include o gamă largă de părți interesate. Mai exact, acest ecosistem include actorii tradiționali din industria autovehiculelor, precum și actorii emergenți din industria digitală. Prin urmare, prezentele orientări se adresează producătorilor de vehicule, producătorilor de echipamente și furnizorilor de componente pentru vehicule, reparatorilor auto, concesionarilor auto, furnizorilor de servicii pentru vehicule, administratorilor de parcuri auto, societăților de asigurări auto, furnizorilor de servicii de divertisment, operatorilor de telecomunicații, administratorilor de infrastructură rutieră și autorităților publice, precum și persoanelor vizate. CEPD subliniază faptul că fiecare serviciu se adresează unor categorii de persoane vizate diferite (de exemplu, conducători auto, proprietari, pasageri etc.). Aceasta este o listă neexhaustivă, deoarece ecosistemul implică o gamă largă de servicii, inclusiv servicii pentru care este necesară autentificarea sau identificarea directă și servicii pentru care acestea nu sunt necesare.

31. Unele prelucrări de date cu caracter personal efectuate de persoane fizice în vehicul se încadrează la prelucrare „în cadrul unei activități exclusiv personale sau domestice” și, prin urmare, nu intră sub incidența RGPD[21]. Acestea se referă în special la utilizarea datelor cu caracter personal în vehicule exclusiv de către persoanele vizate care au furnizat aceste date în tabloul de bord al vehiculului. Totuși, CEPD reamintește faptul că, în temeiul considerentului 18, RGPD „se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice”.

1.3.1 În afara domeniului de aplicare al prezentului document

32. Angajatorii care pun la dispoziția angajaților mașini de serviciu ar putea dori să monitorizeze acțiunile acestora (de exemplu, pentru a asigura siguranța angajaților, a bunurilor sau a vehiculelor, pentru a aloca resurse, pentru a urmări și a factura un serviciu sau pentru a verifica timpul de lucru). Prelucrarea datelor efectuată de angajatori în acest caz aduce în discuție considerente specifice în contextul ocupării forței de muncă, care ar putea fi reglementate de legislația muncii la nivel național ce nu poate fi detaliată în prezentele orientări[22].

33. Deși prelucrarea datelor în contextul vehiculelor comerciale utilizate în scopuri profesionale (cum ar fi transportul public) și al soluției de transport partajat și MaaS (mobilitatea ca serviciu) poate aduce în discuție considerente specifice care nu fac obiectul

[21] A se vedea RGPD, articolul 2 alineatul (2) litera (c).
[22] Grupul de lucru „Articolul 29” a detaliat acest aspect în Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă (WP 249); https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

prezentelor orientări generale, multe dintre principiile și recomandările prezentate în acest document se vor aplica, de asemenea, acestor tipuri de prelucrare.

34. În calitate de sisteme ce comunică prin unde radio, vehiculele conectate fac obiectul localizării pasive, cum ar fi localizarea prin Wi-Fi sau Bluetooth. În acest sens, ele nu diferă de alte dispozitive conectate și intră sub incidența Directivei asupra confidențialității și comunicațiilor electronice, în prezent în curs de revizuire. Prin urmare, este exclusă, de asemenea, urmărirea pe scară largă a vehiculelor echipate cu puncte de acces Wi-Fi[23] de către o rețea extinsă de trecători care utilizează servicii obișnuite de localizare pe smartphone-urile lor. Aceste servicii transmit în mod regulat elementele de identificare ale tuturor rețelelor Wi-Fi vizibile către serverele centrale. Întrucât elementele de identificare ale punctelor de acces Wi-Fi integrate în vehicul pot fi considerate elemente de identificare secundare specifice vehiculului[24], există riscul colectării sistematice, continue, a unor profiluri complete de mișcare a vehiculului.

35. Vehiculele sunt tot mai frecvent echipate cu dispozitive de înregistrare a imaginilor (de exemplu, sisteme de camere video pentru parcare sau camere video instalate la bord). Întrucât se referă la filmarea unor locuri publice, care necesită o evaluare a cadrului legislativ relevant specific fiecărui stat membru, acest tip de prelucrare a datelor nu face obiectul prezentelor orientări.

36. Prelucrarea datelor pentru implementarea sistemelor de transport inteligente cooperative (STI-C), astfel cum sunt definite în Directiva 2010/40/UE[25], a fost abordată de Grupul de lucru „Articolul 29" într-un aviz special[26]. În timp ce definiția conceptului STI-C din directivă nu conține specificații tehnice, Grupul de lucru „Articolul 29" se axează în avizul său pe comunicațiile pe distanțe scurte, care nu implică intervenția unui operator de rețea. Mai precis, acesta analizează cazurile de utilizare specifice elaborate pentru implementarea inițială și s-a angajat să evalueze, într-o etapă ulterioară, noile aspecte care vor fi, fără îndoială, aduse în discuție atunci când se va ajunge la un nivel mai ridicat de automatizare. Întrucât implicațiile legate de protecția datelor în contextul STI-C sunt foarte specifice (cantități fără precedent de date de localizare, transmiterea continuă de date cu caracter personal, schimbul de date între vehicule și alte elemente ale infrastructurii rutiere etc.) și sunt încă în curs de dezbatere la nivel european, prelucrarea datelor cu caracter personal în acest context nu face obiectul prezentelor orientări.

37. În cele din urmă, prezentul document nu urmărește să abordeze toate problemele și întrebările posibile referitoare la vehiculele conectate și, prin urmare, nu poate fi considerat exhaustiv.

1.4 Definiții

38. **Prelucrarea** datelor cu caracter personal cuprinde orice operațiune care implică date cu caracter personal, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere,

[23] Pentru detalii, a se vedea: 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 și Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings (Identificarea vehiculelor pe baza identificatorului secundar al vehiculului - analiză și măsurători în proceduri), VEHICULAR 2017, A șasea conferință internațională privind evoluțiile în sistemele, tehnologiile și aplicațiile vehiculelor, Nisa, Franța, 23-27 iulie 2017, p. 32-37.

[25] Directiva 2010/40/UE din 7 iulie 2020 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport; https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32010L0040&from=RO.

[26] Grupul de lucru „Articolul 29" - Avizul nr. 3/2017 privind prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative (STI-C); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea etc.[27]

39. **Persoana vizată** este persoana fizică la care se referă datele care fac obiectul prelucrării. În contextul vehiculelor conectate, aceasta poate fi, în special, conducătorul auto (principal sau ocazional), pasagerul sau proprietarul vehiculului[28].

40. **Operatorul de date** este persoana care stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal care are loc în vehiculele conectate[29]. Operatorii de date includ furnizorii de servicii care prelucrează datele vehiculului pentru a furniza conducătorului auto informații privind traficul, mesaje privind conducerea ecologică sau alerte referitoare la funcționarea vehiculului, societățile de asigurări care oferă contracte de tipul „Pay As You Drive" sau producătorii de vehicule care colectează date privind uzura pieselor vehiculului în scopul îmbunătățirii calității acestora. În conformitate cu articolul 26 din RGPD, doi sau mai mulți operatori pot stabili în comun scopurile și mijloacele de prelucrare și, prin urmare, pot fi considerați operatori asociați. În acest caz, ei trebuie să își stabilească în mod transparent obligațiile care le revin, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și furnizarea informațiilor prevăzute la articolele 13 și 14 din RGPD.

41. **Persoana împuternicită de operator** este orice persoană care prelucrează datele cu caracter personal pentru și în numele operatorului[30]. Persoana împuternicită de operator colectează și prelucrează datele conform instrucțiunilor operatorului, fără a utiliza datele respective în scopuri proprii. De exemplu, în anumite situații, producătorii de echipamente și furnizorii din sectorul auto pot prelucra date în numele producătorilor de vehicule (ceea ce nu înseamnă că nu pot fi operatori de date în alte scopuri). Articolul 28 din RGPD stabilește obligațiile persoanelor împuternicite de operator și impune acestora să pună în aplicare măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului.

42. **Destinatar** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță[31]. De exemplu, un partener comercial al furnizorului de servicii care primește de la acesta din urmă date cu caracter personal generate de vehicul este un destinatar. Indiferent dacă acționează în calitate de operator nou sau de persoană împuternicită de operator, destinatarul își îndeplinește toate obligațiile care îi revin în temeiul RGPD.

43. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari[32]; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării. De exemplu, autoritățile de aplicare a legii sunt părți terțe autorizate atunci când solicită date cu caracter personal pentru efectuarea unei anchete în conformitate cu dreptul Uniunii sau cel al statelor membre.

[27] A se vedea articolul 4 punctul (2) din RGPD.
[28] A se vedea articolul 4 punctul (1) din RGPD.
[29] A se vedea articolul 4 punctul (7) din RGPD și Comitetul european pentru protecția datelor, Orientările 7/2020 privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD (denumite în continuare „Orientările 7/2020").
[30] A se vedea articolul 4 punctul (8) din RGPD și Orientările 7/2020.
[31] A se vedea articolul 4 punctul (9) din RGPD și Orientările 7/2020.
[32] A se vedea articolul 4 punctul (9) și considerentul 31 din RGPD.

1.5 Riscurile legate de viața privată și protecția datelor cu caracter personal

44. Grupul de lucru „Articolul 29” a exprimat deja o serie de îngrijorări cu privire la sistemele IoT (internetul obiectelor) care se pot aplica și vehiculelor conectate[33]. Aspectele deja subliniate legate de securitatea și controlul datelor în contextul internetului obiectelor sunt chiar mai sensibile în contextul vehiculelor conectate, deoarece implică preocupări legate de siguranța rutieră – și pot afecta integritatea fizică a conducătorului auto – într-un mediu perceput în mod tradițional ca fiind izolat și protejat de interferențe externe.

45. De asemenea, vehiculele conectate generează preocupări majore legate de protecția datelor și viața privată în cazul prelucrării datelor de localizare, deoarece caracterul din ce în ce mai intruziv al acestora poate pune presiune asupra posibilităților actuale de păstrare a anonimatului persoanelor fizice. CEPD dorește să sublinieze în mod special și să sensibilizeze părțile interesate cu privire la faptul că utilizarea tehnologiilor de localizare necesită punerea în aplicare a unor garanții specifice pentru a preveni supravegherea persoanelor fizice și utilizarea abuzivă a datelor.

1.5.1 Lipsa controlului și asimetria informațiilor

46. Este posibil ca șoferii și pasagerii vehiculelor să nu fie întotdeauna informați în mod adecvat cu privire la prelucrarea datelor care are loc în sau prin intermediul unui vehicul conectat. Este posibil ca informațiile să fie furnizate doar proprietarului vehiculului, care poate să nu fie conducătorul auto, și să nu fie furnizate în timp util. Prin urmare, există riscul să nu fie oferite suficiente funcționalități sau opțiuni pentru exercitarea controlului necesar astfel încât persoanele afectate să facă uz de drepturile lor privind protecția datelor cu caracter personal și viața privată. Acest aspect este important deoarece, pe durata lor de viață, vehiculele pot aparține mai multor proprietari, fie pentru că sunt vândute sau fac mai degrabă obiectul unui contract de leasing (nu de vânzare-cumpărare).

47. De asemenea, comunicarea în vehicul poate fi inițiată atât automat, cât și în mod implicit, fără ca persoana să aibă cunoștință de acest lucru. În absența posibilității de a controla în mod eficace modul în care vehiculul și echipamentele conectate la acesta interacționează, fluxul de date va fi, în mod inevitabil, extrem de dificil de controlat de către utilizator. Controlul utilizării ulterioare a acestui flux de date și, prin urmare, evitarea unei eventuale denaturări a funcțiilor vor fi chiar mai dificil de realizat.

1.5.2 Calitatea consimțământului utilizatorului

48. CEPD subliniază faptul că, atunci când prelucrarea datelor cu caracter personal are la bază consimțământul persoanei vizate, trebuie îndeplinite toate elementele consimțământului valabil, adică să fie o manifestare de voință liber exprimată, specifică, în cunoștință de cauză și lipsită de ambiguitate, conform orientărilor CEPD privind consimțământul[34]. Operatorii de date trebuie să acorde o atenție deosebită modalităților de obținere a consimțământului valabil din partea diferiților participanți, cum ar fi proprietarii sau utilizatorii vehiculelor. Consimțământul trebuie să fie acordat separat, în scopuri specifice și nu poate fi asociat executării contractului de vânzare-cumpărare sau de leasing al unui automobil nou. Consimțământul trebuie să poată fi retras cu aceeași ușurință cu care a fost acordat.

49. Același lucru este valabil și în cazul în care exprimarea consimțământului este necesară pentru respectarea dispozițiilor Directivei asupra confidențialității și comunicațiilor

[33] Grupul de lucru „Articolul 29” – Avizul 8/2014 privind evoluțiile recente din sfera internetului obiectelor; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_ro.pdf.
[34] Comitetul european pentru protecția datelor, Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, Versiunea 1.1, 4 mai 2020 (denumite în continuare „Orientările 05/2020”).

electronice, de exemplu, în cazul stocării de informații sau al accesării informațiilor deja stocate în vehicul, astfel cum se prevede în anumite cazuri la articolul 5 alineatul (3) din directiva menționată. Într-adevăr, astfel cum s-a subliniat mai sus, consimțământul în acest context trebuie interpretat în temeiul RGPD.

50. De multe ori, este posibil ca utilizatorul să nu aibă cunoștință de prelucrarea datelor cu caracter personal efectuată în vehiculul său. Lipsa acestei informații constituie un obstacol major în calea demonstrării consimțământului valabil în temeiul RGPD, întrucât acesta trebuie să fie exprimat în cunoștință de cauză. În astfel de situații, consimțământul nu poate fi utilizat ca temei juridic pentru respectiva prelucrare a datelor cu caracter personal în temeiul RGPD.

51. Este posibil ca mecanismele clasice utilizate pentru a obține consimțământul persoanelor fizice să fie dificil de aplicat în contextul vehiculelor conectate, ceea ce duce la un consimțământ „de slabă calitate" bazat pe o lipsă de informații sau la imposibilitatea faptică de a asigura un consimțământ adaptat preferințelor exprimate de persoanele fizice. De asemenea, consimțământul ar putea fi dificil de obținut în practică de la conducătorii auto și pasagerii care nu au legătură cu proprietarul vehiculului, cum ar fi în cazul vehiculelor de ocazie, închiriate printr-un contract de leasing sau de închiriere, sau împrumutate.

52. Totuși, atunci când Directiva privind viața privată și comunicațiile electronice nu prevede obținerea consimțământului persoanei vizate, operatorul trebuie să aleagă temeiul juridic de la articolul 6 din RGPD care este cel mai adecvat pentru prelucrarea datelor cu caracter personal.

1.5.3 Prelucrarea ulterioară a datelor cu caracter personal

53. Atunci când datele sunt colectate pe baza consimțământului în conformitate cu articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice sau pe baza uneia dintre excepțiile de la articolul 5 alineatul (3) și sunt prelucrate ulterior în conformitate cu articolul 6 din RGPD, această prelucrare ulterioară poate avea loc numai dacă operatorul obține un nou consimțământ exprimat de persoana vizată în acest alt scop sau dacă poate demonstra că prelucrarea se bazează pe dreptul Uniunii sau dreptul intern al statului membru în scopul de a garanta atingerea obiectivelor menționate la articolul 23 alineatul (1) din RGPD[35]. CEPD consideră că prelucrarea ulterioară pe baza unui test de compatibilitate în conformitate cu articolul 6 alineatul (4) din RGPD nu este posibilă în astfel de cazuri, deoarece ar submina standardul privind protecția datelor prevăzut în Directiva privind viața privată și comunicațiile electronice. Într-adevăr, consimțământul, atunci când este necesar în temeiul Directivei privind viața privată și comunicațiile electronice, trebuie să fie specific și exprimat în cunoștință de cauză, ceea ce înseamnă că persoanele vizate trebuie să cunoască fiecare scop în care sunt prelucrate datele cu caracter personal și să aibă dreptul de a refuza prelucrarea în scopuri specifice[36]. A considera că prelucrarea ulterioară pe baza unui test de compatibilitate în conformitate cu articolul 6 alineatul (4) din RGPD este posibilă ar eluda principiul însuși al cerințelor privind consimțământul prevăzute în actuala directivă.

54. CEPD reamintește faptul că prelucrarea ulterioară nu poate fi efectuată pe baza consimțământului inițial, deoarece consimțământul trebuie să fie exprimat în cunoștință de cauză și specific pentru a fi valabil.

[35] A se vedea, de asemenea, Comitetul european pentru protecția datelor, Orientările 10/2020 privind restricțiile în temeiul articolului 23 din RGPD.
[36] Orientările 05/2020, secțiunile 3.2 și 3.3.

55. De exemplu, datele telemetrice, care sunt colectate în timpul utilizării vehiculului în scopuri de întreținere, nu pot fi divulgate societăților de asigurări auto fără consimțământul utilizatorilor în scopul creării de profiluri ale conducătorilor auto pentru a oferi polițe de asigurare bazate pe stilul de conducere.

56. În plus, datele colectate de vehiculele conectate pot fi prelucrate de autoritățile de aplicare a legii pentru a detecta excesul de viteză sau alte încălcări ale legislației dacă și când sunt îndeplinite condițiile specifice din Directiva privind aplicarea legii. În acest caz, aceste date vor fi considerate ca fiind date referitoare la condamnări penale și infracțiuni în condițiile prevăzute la articolul 10 din RGPD și în orice legislație națională aplicabilă. Producătorii pot furniza astfel de date autorităților de aplicare a legii în cazul în care sunt îndeplinite condițiile specifice pentru o astfel de prelucrare. CEPD subliniază faptul că prelucrarea datelor cu caracter personal numai cu scopul de a da curs cererilor formulate de autoritățile de aplicare a legii nu constituie un scop determinat, explicit și legitim în sensul articolului 5 alineatul (1) litera (b) din RGPD. Atunci când sunt autorizate prin lege, aceste autorități ar putea fi părți terțe în sensul articolului 4 punctul (10) din RGPD; în acest caz, producătorii ar avea dreptul de a le furniza orice date de care dispun, sub rezerva respectării cadrului juridic relevant din fiecare stat membru.

1.5.4 Colectarea excesivă a datelor

57. Având în vedere numărul tot mai mare de senzori montați pe vehiculele conectate, există un risc foarte ridicat de colectare excesivă a datelor față de ceea ce este necesar pentru îndeplinirea scopului.

58. Dezvoltarea de noi funcționalități și, mai exact, a celor bazate pe algoritmi de învățare automată poate necesita colectarea unui volum mare de date pe o perioadă lungă de timp.

1.5.5 Securitatea datelor cu caracter personal

59. Numărul mare de funcționalități, servicii și interfețe (de exemplu, internet, USB, RFID, Wi-Fi) oferite de vehiculele conectate crește suprafața de atac și, prin urmare, numărul de vulnerabilități potențiale prin care datele cu caracter personal ar putea fi compromise. Spre deosebire de majoritatea dispozitivelor IoT, vehiculele conectate sunt sisteme critice în care o încălcare a securității poate pune în pericol viața utilizatorilor și a persoanelor din jur. Prin urmare, abordarea riscului ca hackerii să încerce să profite de vulnerabilitățile vehiculelor conectate este deosebit de importantă.

60. În plus, datele cu caracter personal stocate în vehicule și/sau în locuri externe (de exemplu, în infrastructurile de cloud computing) trebuie protejate în mod corespunzător împotriva accesului neautorizat. De exemplu, pentru efectuarea lucrărilor de întreținere, un vehicul trebuie să fie predat unui tehnician care va solicita acces la unele date tehnice ale vehiculului. Deși tehnicianul are nevoie de acces la respectivele date tehnice, este posibil ca acesta să încerce să acceseze toate datele stocate în vehicul.

2 RECOMANDĂRI GENERALE

61. Pentru a reduce riscurile pentru persoanele vizate identificate mai sus, producătorii de vehicule și echipamente, furnizorii de servicii sau orice altă parte interesată care ar putea acționa în calitate de operator sau de persoană împuternicită de operator în legătură cu vehiculele conectate ar trebui să respecte următoarele recomandări generale.

2.1 Categorii de date

62. Astfel cum s-a menționat în introducere, majoritatea datelor legate de vehiculele conectate vor fi considerate date cu caracter personal în măsura în care pot fi asociate cu una sau mai multe persoane identificabile. Acestea includ date tehnice privind deplasarea vehiculului (de exemplu, viteza, distanța parcursă), precum și starea acestuia (de exemplu,

temperatura lichidului de răcire a motorului, turația motorului, presiunea în pneuri). Anumite date generate de vehiculele conectate pot necesita, de asemenea, o atenție deosebită, având în vedere sensibilitatea acestora și/sau impactul potențial asupra drepturilor și intereselor persoanelor vizate. În prezent, CEPD a identificat trei categorii de date cu caracter personal care necesită o atenție specială din partea producătorilor de vehicule și echipamente, a furnizorilor de servicii și a altor operatori de date: date de localizare, date biometrice (și orice categorie specială de date conform articolului 9 din RGPD) și date care ar putea dezvălui infracțiuni sau încălcări ale normelor de circulație rutieră.

2.1.1 Date de localizare

63. Atunci când colectează date cu caracter personal, producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date ar trebui să țină cont de faptul că datele de localizare dezvăluie în mare măsură obiceiurile de viață ale persoanelor vizate. Călătoriile efectuate au un caracter specific deoarece permit deducerea locului de muncă și a domiciliului, precum și a intereselor conducătorului auto (activități de recreere), și pot dezvălui informații sensibile, cum ar fi convingerile religioase, prin locașurile de cult frecventate, sau orientarea sexuală, prin locurile vizitate. Prin urmare, producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date ar trebui să fie deosebit de precauți și să nu colecteze date de localizare decât dacă acest lucru este absolut necesar în raport cu scopul prelucrării. De exemplu, atunci când prelucrarea constă în detectarea deplasării vehiculului, giroscopul este suficient pentru a îndeplini această funcție, fără a fi necesară colectarea datelor de localizare.

64. În general, colectarea datelor de localizare trebuie să respecte următoarele principii:

- configurarea adecvată a frecvenței de accesare și a nivelului de detaliu al datelor de localizare colectate în raport cu scopul prelucrării. De exemplu, o aplicație privind starea vremii nu ar trebui să aibă acces la amplasarea vehiculului în fiecare secundă, chiar dacă persoana vizată și-a exprimat consimțământul în acest sens;
- furnizarea de informații exacte cu privire la scopul prelucrării (de exemplu, este stocat istoricul locațiilor? Dacă da, care este scopul acestuia?);
- atunci când prelucrarea se bazează pe consimțământul persoanei vizate, obținerea unui consimțământ valabil (liber exprimat, specific și în cunoștință de cauză), care este diferit de condițiile generale de vânzare sau de utilizare, de exemplu pe computerul de bord;
- activarea localizării numai atunci când utilizatorul lansează o funcționalitate care necesită cunoașterea poziției vehiculului și nu în mod implicit și continuu atunci când vehiculul este pornit;
- informarea utilizatorului cu privire la faptul că funcția de localizare a fost activată, în special prin utilizarea de pictograme (de exemplu, o săgeată care se deplasează pe ecran);
- opțiunea de a dezactiva în orice moment funcția de localizare;
- definirea unei perioade limitate de stocare.

2.1.2 Date biometrice

65. În contextul vehiculelor conectate, datele biometrice utilizate în scopul identificării unice a unei persoane fizice pot fi prelucrate, în conformitate cu articolul 9 din RGPD și cu excepțiile naționale, printre altele, pentru a permite accesul la un vehicul, pentru autentificarea conducătorului auto/proprietarului și/sau pentru a permite accesul la setările și preferințele asociate profilului conducătorului auto. Atunci când se are în vedere utilizarea datelor biometrice, garantarea controlului deplin al persoanei vizate asupra datelor sale implică, pe de o parte, existența unei alternative nebiometrice (de exemplu,

utilizarea unei chei fizice sau a unui cod) fără constrângeri suplimentare (și anume, utilizarea biometriei nu ar trebui să fie obligatorie) și, pe de altă parte, stocarea și compararea modelului biometric în formă criptată doar la nivel local, datele biometrice nefiind prelucrate de un terminal de citire/comparare extern.

66. În cazul datelor biometrice[37], este importantă asigurarea faptului că soluția de autentificare biometrică este suficient de fiabilă, în special prin respectarea următoarelor principii:

- soluția biometrică utilizată (de exemplu, rata rezultatelor fals pozitive și fals negative) este adaptată la nivelul de securitate al controlului necesar al accesului;
- soluția biometrică utilizată se bazează pe un senzor rezistent la atacuri (cum ar fi utilizarea unei amprente digitale imprimate plat pentru recunoașterea amprentelor digitale);
- numărul încercărilor de autentificare este limitat;
- modelul biometric este stocat în vehicul într-o formă criptată utilizând un algoritm de criptare și o gestionare a cheilor de criptare care reflectă stadiul actual al tehnologiei;
- datele brute utilizate pentru crearea modelului biometric și pentru autentificarea utilizatorului sunt prelucrate în timp real, fără a fi stocate, nici măcar la nivel local.

2.1.3 Date referitoare la infracțiuni sau alte încălcări ale dispozițiilor legale

67. Pentru prelucrarea datelor referitoare la posibile infracțiuni în sensul articolului 10 din RGPD, CEPD recomandă să se recurgă la prelucrarea locală a datelor, unde persoana vizată are un control deplin asupra prelucrării respective (a se vedea discuția privind prelucrarea locală din secțiunea 2.4). Într-adevăr, cu unele excepții (a se vedea studiile de accidentologie prezentate în secțiunea 3.3 de mai jos), prelucrarea externă a datelor referitoare la infracțiuni sau alte încălcări ale dispozițiilor legale este interzisă. Astfel, în funcție de sensibilitatea datelor, este necesară punerea în aplicare a unor măsuri de securitate eficiente, precum cele descrise la secțiunea 2.7, pentru a asigura protecția împotriva accesului, a modificării și a ștergerii neautorizate a acestor date.

68. Într-adevăr, unele categorii de date cu caracter personal generate de vehiculele conectate ar putea indica faptul că o infracțiune sau o altă încălcare a dispozițiilor legale a fost sau este săvârșită („date referitoare la infracțiuni”) și, prin urmare, ar putea face obiectul unor restricții speciale (de exemplu, date care indică faptul că vehiculul a depășit o linie continuă, viteza instantanee a vehiculului combinată cu date de localizare precise). În cazul în care astfel de date ar fi prelucrate de autoritățile naționale competente în scopul investigării unei infracțiuni și al urmăririi penale, s-ar aplica garanțiile prevăzute la articolul 10 din RGPD.

2.2 Scopuri

69. Datele cu caracter personal pot fi prelucrate într-o gamă variată de scopuri în contextul vehiculelor conectate, inclusiv siguranța conducătorului auto, asigurare, transport eficient, servicii de divertisment sau informații. În conformitate cu RGPD, operatorii trebuie să colecteze date cu caracter personal în scopuri „determinate, explicite și legitime”, să se asigure că datele nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri și că prelucrarea se bazează pe un temei juridic valabil, astfel cum se prevede la articolul 5 din RGPD. Unele exemple concrete de scopuri care pot fi urmărite de operatorii de date în contextul vehiculelor conectate sunt discutate în partea III a prezentelor orientări, alături de recomandări specifice pentru fiecare tip de prelucrare.

[37] Principiul interzicerii prevăzut la articolul 9 alineatul (1) din RGPD se referă numai la „date[le] biometrice pentru identificarea unică a unei persoane fizice”.

2.3 Relevanța și reducerea la minimum a datelor

70. Pentru a respecta principiul reducerii la minimum a datelor[38], producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date trebuie să acorde o atenție deosebită categoriilor de date de care au nevoie de la un vehicul conectat, având în vedere că trebuie să colecteze doar acele date cu caracter personal care sunt relevante și necesare pentru scopul în care sunt prelucrate. De exemplu, datele de localizare sunt deosebit de intruzive și pot dezvălui multe obiceiuri de viață ale persoanelor vizate. Prin urmare, actorii din acest sector ar trebui să fie deosebit de precauți și să nu colecteze date de localizare decât dacă acest lucru este absolut necesar în raport cu scopul prelucrării (a se vedea discuția privind datele de localizare din secțiunea 2.1 de mai sus).

2.4 Protecția datelor începând cu momentul conceperii și în mod implicit

71. Ținând cont de volumul și diversitatea datelor cu caracter personal generate de vehiculele conectate, CEPD menționează faptul că operatorii de date au obligația de a se asigura că tehnologiile utilizate în contextul vehiculelor conectate sunt configurate astfel încât să respecte viața privată a persoanelor fizice prin aplicarea obligațiilor de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit, astfel cum se prevede la articolul 25 din RGPD. Tehnologiile ar trebui să fie concepute astfel încât să reducă la minimum colectarea datelor cu caracter personal, să ofere setări implicite pentru protecția vieții private și să asigure faptul că persoanele vizate sunt bine informate și au opțiunea de a modifica cu ușurință configurațiile asociate cu datele cu caracter personal care le privesc. Elaborarea unor orientări specifice privind modul în care producătorii și furnizorii de servicii pot respecta obligația de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit ar putea fi benefică pentru industrie și furnizorii terți de aplicații.

72. Unele practici generale, descrise mai jos, pot contribui, de asemenea, la reducerea riscurilor pentru drepturile și libertățile persoanelor fizice în contextul vehiculelor conectate[39].

2.4.1 Prelucrarea locală a datelor cu caracter personal

73. În general, producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date ar trebui, ori de câte ori este posibil, să utilizeze procese care nu implică date cu caracter personal sau transferul unor astfel de date în afara vehiculului (și anume, datele să fie prelucrate intern). Cu toate acestea, natura vehiculelor conectate prezintă unele riscuri, cum ar fi posibilitatea unor atacuri asupra prelucrării locale de către actori externi sau scurgerea de date locale prin vânzarea pieselor vehiculului. Prin urmare, ar trebui să se acorde atenția cuvenită și luate măsurile de securitate adecvate pentru asigurarea faptului că prelucrarea locală rămâne locală. Acest scenariu oferă avantajul de a garanta utilizatorului controlul exclusiv și deplin asupra datelor sale cu caracter personal și, ca atare, prezintă, „începând cu momentul conceperii", mai puține riscuri la adresa vieții private, în special prin interzicerea oricărei prelucrări de date de către părțile interesate fără informarea persoanei vizate. Acesta permite, de asemenea, prelucrarea datelor sensibile, cum ar fi datele biometrice sau datele referitoare la infracțiuni sau alte încălcări ale dispozițiilor legale, precum și a datelor de localizare detaliate care, în caz contrar, ar face obiectul unor norme mai stricte (a se vedea mai jos). În aceeași ordine de idei, această soluție prezintă mai puține riscuri pentru securitatea cibernetică și implică o perioadă de

[38] Articolul 5 alineatul (1) litera (c) din RGPD.

[39] A se vedea și Comitetul european pentru protecția datelor, Orientările nr. 4/2019 privind articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, Versiunea 2.0, adoptate la 20 octombrie 2020 (denumite în continuare „Orientările nr. 4/2019").

latență redusă, fiind astfel adecvată în mod special pentru funcțiile automatizate de asistență la conducere. Mai jos sunt prezentate câteva exemple pentru acest tip de soluție:

- aplicații de conducere ecologică care prelucrează date în vehicul pentru a afișa în timp real recomandări pentru o conducere ecologică pe ecranul de la bordul vehiculului;
- aplicații care implică transferul de date cu caracter personal către un dispozitiv, cum ar fi un smartphone, aflat sub controlul deplin al utilizatorului (de exemplu, prin Bluetooth sau Wi-Fi) și în care datele vehiculului nu sunt transmise furnizorilor de aplicații sau producătorilor de vehicule; acestea includ, de exemplu, cuplarea smartphone-urilor pentru a utiliza ecranul de la bordul vehiculului, sistemele multimedia, microfonul (sau alți senzori) pentru apeluri telefonice etc., în măsura în care datele colectate rămân sub controlul persoanei vizate și sunt utilizate exclusiv pentru furnizarea serviciului solicitat;
- aplicații de sporire a siguranței la bordul vehiculului, cum ar fi cele care emit semnale sonore sau vibrații ale volanului atunci când conducătorul auto depășește un alt vehicul fără a semnaliza sau trece peste o linie continuă, sau care emit alerte cu privire la starea vehiculului (de exemplu, o avertizare cu privire la uzura plăcuțelor de frână);
- aplicații pentru deblocarea, pornirea și/sau activarea anumitor comenzi ale vehiculului care utilizează datele biometrice ale conducătorului auto stocate în vehicul (cum ar fi modele faciale sau vocale sau puncte caracteristice ale amprentelor digitale).

74. Aplicații precum cele menționate mai sus implică prelucrarea datelor cu caracter personal de către o persoană fizică în cadrul unor activități exclusiv personale (și anume, fără ca aceste date să fie transferate către un operator sau o persoană împuternicită de operator). Prin urmare, în conformitate cu articolul 2 alineatul (2) din RGPD, **aceste aplicații nu intră sub incidența RGPD.**

75. Cu toate acestea, dacă RGPD nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice, regulamentul se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice (producători de vehicule, furnizori de servicii etc.) conform considerentului 18 din RGPD. Prin urmare, atunci când acționează în calitate de operator sau persoană împuternicită de operator, aceștia trebuie să dezvolte o aplicație securizată la bordul vehiculului, respectând principiul protejării vieții private începând cu momentul conceperii și în mod implicit. În orice caz, conform considerentului 78 din RGPD, „[a]tunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor”[40]. Pe de o parte, acest lucru va consolida dezvoltarea serviciilor centrate pe utilizator și, pe de altă parte, va facilita și va asigura orice alte utilizări viitoare care ar putea intra în domeniul de aplicare al RGPD. Mai precis, CEPD recomandă dezvoltarea unei platforme securizate de aplicații la bordul vehiculului, separată fizic de funcțiile de siguranță ale acestuia, astfel încât accesul la datele vehiculului să nu depindă de capacitățile cloud externe nenecesare.

[40] Pentru mai multe recomandări privind protejarea vieții private începând cu momentul conceperii și protejarea implicită a vieții private, a se vedea, de asemenea, Orientările nr. 4/2019.

76. Producătorii de vehicule și furnizorii de servicii ar trebui să aibă în vedere prelucrarea locală a datelor cu caracter personal, ori de câte ori este posibil, pentru a reduce riscurile potențiale ale prelucrării în cloud, astfel cum se subliniază în Avizul Grupului de lucru „Articolul 29" privind „cloud computing"[41].

77. În general, utilizatorii ar trebui să poată controla modul în care datele lor sunt colectate și prelucrate în vehicul:

- informațiile privind prelucrarea trebuie să fie furnizate în limba conducătorului auto (manual, setări etc.);
- CEPD recomandă prelucrarea implicită doar a datelor strict necesare pentru funcționarea vehiculului. Persoanele vizate ar trebui să aibă posibilitatea de a activa sau a dezactiva prelucrarea datelor pentru orice alt scop și operator/persoană împuternicită de operator și de a șterge datele în cauză, ținând cont de scopul și temeiul juridic al prelucrării datelor cu caracter personal;
- datele nu ar trebui transmise niciunui terț (utilizatorul are acces exclusiv la date);
- datele ar trebui păstrate numai atât timp cât este necesar pentru prestarea serviciului sau pe o perioadă prevăzută în alt mod în dreptul Uniunii sau dreptul intern;
- persoanele vizate ar trebui să aibă posibilitatea de a șterge definitiv orice date cu caracter personal înainte ca vehiculele să fie puse în vânzare;
- persoanele vizate ar trebui, atunci când este posibil, să aibă acces direct la datele generate de aceste aplicații.

78. În fine, întrucât prelucrarea locală a datelor cu caracter personal nu este întotdeauna posibilă pentru fiecare caz de utilizare, de multe ori „prelucrarea hibridă" poate fi o soluție. De exemplu, în contextul asigurărilor bazate pe utilizare, datele cu caracter personal referitoare la comportamentul conducătorului auto (cum ar fi forța cu care este apăsată pedala de frână, numărul de kilometri parcurși etc.) ar putea fi prelucrate fie în interiorul vehiculului, fie de către furnizorul de servicii telematice în numele societății de asigurări (operatorul de date) pentru a genera punctaje numerice care sunt transferate societății de asigurări în mod regulat (de exemplu, lunar). Astfel, societatea de asigurări nu are acces la datele brute privind comportamentul conducătorului auto, ci doar la punctajul agregat rezultat în urma prelucrării. Acest lucru asigură respectarea principiilor de reducere la minimum a datelor începând cu momentul conceperii. Aceasta înseamnă și că utilizatorii trebuie să aibă posibilitatea de a-și exercita drepturile în cazul stocării datelor de către alte părți: de exemplu, un utilizator ar trebui să aibă posibilitatea de a șterge datele stocate în sistemele unui atelier de service sau ale unui concesionar auto în condițiile prevăzute la articolul 17 din RGPD.

2.4.2 Anonimizarea și pseudonimizarea

79. În cazul în care se are în vedere transmiterea de date cu caracter personal în afara vehiculului, ar trebui să se ia în considerare anonimizarea acestora înainte de transferul propriu-zis. Pentru anonimizarea datelor, operatorul ar trebui să ia în considerare toate prelucrările care ar putea duce la reidentificarea datelor, cum ar fi transmiterea de date anonimizate la nivel local. CEPD reamintește faptul că principiile protecției datelor nu se aplică informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel

[41] Grupul de lucru „Articolul 29" – Avizul nr. 5/2012 privind „cloud computing"; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_ro.pdf.

încât persoana vizată nu este sau nu mai este identificabilă[42]. După ce un set de date este cu adevărat anonimizat, iar persoanele fizice nu mai sunt identificabile, legislația europeană privind protecția datelor nu se mai aplică. În consecință, anonimizarea, dacă este cazul, poate fi o bună strategie de păstrare a beneficiilor și de reducere a riscurilor în contextul vehiculelor conectate.

80. După cum se detaliază în avizul Grupului de lucru „Articolul 29" privind tehnicile de anonimizare, pentru anonimizarea datelor pot fi utilizate diferite metode, uneori în combinație[43].

81. Alte tehnici, cum ar fi pseudonimizarea[44], pot contribui la reducerea la minimum a riscurilor generate de prelucrarea datelor cu caracter personal, ținând cont de faptul că, în majoritatea cazurilor, datele identificabile în mod direct nu sunt necesare pentru îndeplinirea scopului prelucrării. Dacă este sprijinită de garanții de securitate, pseudonimizarea asigură o protecție sporită a datelor cu caracter personal prin reducerea riscurilor de utilizare abuzivă. Pseudonimizarea este reversibilă, spre deosebire de anonimizare, iar datele pseudonimizate sunt considerate date cu caracter personal care fac obiectul RGPD.

2.4.3 Evaluări ale impactului asupra protecției datelor

82. Având în vedere volumul și sensibilitatea datelor cu caracter personal care pot fi generate în contextul vehiculelor conectate, este posibil ca prelucrarea, în special în situațiile în care datele cu caracter personal sunt prelucrate în afara vehiculului, să genereze adesea un risc ridicat pentru drepturile și libertățile persoanelor fizice. Dacă există acest risc, actorii din sectorul autovehiculelor trebuie să realizeze o evaluare a impactului asupra protecției datelor (EIPD) pentru a identifica și a reduce riscurile, astfel cum se detaliază la articolele 35 și 36 din RGPD. Chiar și în cazurile în care nu se impune o evaluare a impactului asupra protecției datelor, se recomandă realizarea unei astfel de evaluări cât mai devreme posibil în procesul de proiectare. Acest lucru va permite actorilor din acest sector să ia în considerare rezultatele acestei analize în procesul de proiectare, înainte de lansarea de noi tehnologii.

2.5 Informare

83. Înainte de prelucrarea datelor cu caracter personal, persoana vizată este informată cu privire la identitatea operatorului (de exemplu, producătorul de vehicule și echipamente sau furnizorul de servicii), scopul prelucrării, destinatarii datelor, perioada pentru care vor fi stocate datele și drepturile persoanei vizate în temeiul RGPD[45].

84. În plus, producătorul de vehicule și echipamente, furnizorul de servicii sau un alt operator de date trebuie să furnizeze persoanei vizate următoarele informații, utilizând un limbaj clar, simplu și într-o formă ușor accesibilă:

- datele de contact ale responsabilului cu protecția datelor;
- scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;

[42] A se vedea articolul 4 punctul (1) și considerentul 26 din RGPD.
[43] WP29 - Avizul 05/2014 privind tehnicile de anonimizare; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_ro.pdf.
[44] Articolul 4 punctul (5) din RGPD. Raportul ENISA din 3 decembrie 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] Articolul 5 alineatul (1) litera (a) și articolul 13 din RGPD. A se vedea, de asemenea, Grupul de lucru „Articolul 29", Orientări privind transparența în temeiul Regulamentului 2016/679 (wp260rev.01), aprobate de CEPD.

- menționarea explicită a intereselor legitime urmărite de operatorul de date sau de un terț, atunci când aceste interese legitime constituie temeiul juridic al prelucrării;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia, atunci când prelucrarea se bazează pe consimțământul persoanei vizate;
- dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și garanțiile utilizate pentru transferul acestora;
- dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- existența unui proces decizional automatizat incluzând crearea de profiluri care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. Acest lucru se poate aplica în special furnizării de asigurări bazate pe utilizare persoanelor fizice;
- dreptul de a depune o plângere în fața unei autorități de supraveghere;
- informații privind prelucrarea ulterioară.
- În cazul mai multor operatori de date, informații clare și complete cu privire la responsabilitățile fiecărui operator.

85. În unele cazuri, datele cu caracter personal nu sunt colectate direct de la persoana vizată. De exemplu, un producător de vehicule și echipamente se poate baza pe un concesionar auto pentru a colecta informații despre proprietarul vehiculului în vederea furnizării unui serviciu de asistență rutieră de urgență. În cazul în care datele nu au fost colectate direct de la persoana vizată, producătorul de vehicule și echipamente, furnizorul de servicii sau un alt operator de date indică, de asemenea, pe lângă informațiile menționate mai sus, categoriile de date cu caracter personal în cauză, sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public. Aceste informații trebuie furnizate de operator într-un termen rezonabil după obținerea datelor și **cel târziu până la prima dintre următoarele date**, în conformitate cu articolul 14 alineatul (3) din RGPD: (i) o lună după obținerea datelor, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal, (ii) în momentul primei comunicări către persoana vizată respectivă sau (iii) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, înainte de transmiterea acestora.

86. De asemenea, ar putea fi necesară furnizarea de informații noi persoanelor vizate în cazul unui operator nou. Un serviciu de asistență rutieră care interacționează cu vehicule conectate poate fi furnizat de operatori de date diferiți, în funcție de țara sau regiunea în care este necesară asistența. Noii operatori ar trebui să furnizeze persoanelor vizate

informațiile necesare atunci când acestea trec frontiera și serviciile care interacționează cu vehiculele conectate sunt furnizate de operatori noi.

87. Informațiile destinate persoanelor vizate pot fi furnizate pe straturi[46], și anume prin separarea a două niveluri de informații: pe de o parte, informațiile de la primul nivel, care sunt cele mai importante pentru persoanele vizate, și, pe de altă parte, informațiile despre care se presupune că prezintă interes într-o etapă ulterioară. Primul nivel de informații esențiale include, pe lângă identitatea operatorului, scopul prelucrării și o descriere a drepturilor persoanei vizate, precum și orice informații suplimentare cu privire la prelucrarea cu cel mai puternic impact asupra persoanei vizate și prelucrarea care ar putea surprinde persoana vizată. CEPD recomandă ca, în contextul vehiculelor conectate, persoana vizată să fie informată cu privire la toți destinatarii în cadrul primului strat de informații. Astfel cum se menționează în Orientările privind transparența elaborate de Grupul de lucru „Articolul 29", operatorii trebuie să furnizeze informații cu privire la destinatari, care sunt cele mai semnificative pentru persoanele vizate. În practică, aceștia vor fi numiți, în general, destinatari, astfel încât persoanele vizate să știe exact cine deține datele lor cu caracter personal. Dacă operatorii nu pot furniza numele destinatarilor, informațiile ar trebui să fie cât mai precise, indicând tipul de destinatari (și anume, prin trimitere la activitățile pe care le desfășoară aceștia), industria, sectorul și subsectorul, precum și localizarea destinatarilor.

88. Persoanele vizate pot fi informate prin clauze concise și ușor de înțeles în contractul de vânzare-cumpărare al vehiculului, în contractul de prestări servicii și/sau în orice mijloc scris, utilizând documente diferite (de exemplu, cartea de întreținere sau manualul de utilizare a vehiculului) sau computerul de bord.

89. Informațiile necesare prevăzute la articolele 13 și 14 din RGPD pot fi furnizate în combinație cu pictograme standardizate, pentru a spori transparența prin posibila reducere a necesității de a transmite persoanei vizate volume mari de informații scrise. Acestea ar trebui să fie vizibile în vehicule pentru a oferi într-un mod inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. CEPD subliniază importanța standardizării acestor pictograme, astfel încât utilizatorul să găsească aceleași simboluri indiferent de marca sau modelul vehiculului. De exemplu, atunci când se colectează anumite tipuri de date, cum ar fi date de localizare, un semnal clar ar putea fi prevăzut la bord (cum ar fi o lumină în interiorul vehiculului) pentru a informa pasagerii cu privire la colectarea acestor date.

2.6 Drepturile persoanei vizate

90. Producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date ar trebui să faciliteze controlul persoanelor vizate asupra datelor care le privesc pe parcursul întregii perioade de prelucrare, prin implementarea unor instrumente specifice prin care acestea își pot exercita drepturile în mod eficace, în special dreptul de acces, dreptul la rectificarea și la ștergerea datelor, dreptul la restricționarea prelucrării și, în funcție de temeiul juridic al prelucrării, dreptul la portabilitatea datelor și dreptul la opoziție.

91. Pentru a facilita modificarea setărilor, ar trebui pus în aplicare un sistem de gestionare a profilurilor pentru a stoca preferințele conducătorilor auto cunoscuți și a-i ajuta să își schimbe cu ușurință setările de confidențialitate în orice moment. Acest sistem de gestionare a profilului ar trebui să centralizeze toate setările datelor pentru fiecare prelucrare, în special pentru a facilita accesul, ștergerea, eliminarea și portabilitatea datelor cu caracter personal din sistemele vehiculului, la cererea persoanei vizate.

[46] A se vedea Grupul de lucru „Articolul 29", Orientări privind transparența în temeiul Regulamentului 2016/679 (wp260rev.01), aprobate de CEPD.

Conducătorii auto ar trebui să aibă posibilitatea de a întrerupe în orice moment colectarea anumitor tipuri de date, temporar sau permanent, cu excepția cazului în care există un temei juridic specific pe care operatorul îl poate invoca pentru a continua colectarea anumitor date. În cazul unui contract care include o ofertă personalizată bazată pe stilul de conducere, acest lucru poate însemna că utilizatorul ar trebui să revină la condițiile standard ale contractului respectiv. Aceste funcții ar trebui implementate în interiorul vehiculului, deși ar putea fi puse la dispoziția persoanelor vizate și prin alte mijloace (de exemplu, o aplicație dedicată). În plus, CEPD recomandă producătorilor să ofere o funcționalitate simplă (cum ar fi un buton de ștergere) pentru a permite persoanelor vizate să șteargă rapid și ușor datele cu caracter personal care pot fi stocate pe tabloul de bord al vehiculului (de exemplu, istoricul de navigație GPS, navigarea pe internet etc.

92. Vânzarea unui vehicul conectat și, prin urmare, transferul dreptului de proprietate ar trebui, de asemenea, să determine ștergerea oricăror date cu caracter personal, care nu mai sunt necesare în scopurile specificate inițial, iar persoana vizată ar trebui să își poată exercita dreptul la portabilitatea datelor.

2.7 Securitate

93. Producătorii de vehicule și echipamente, furnizorii de servicii și alți operatori de date ar trebui să implementeze măsuri care să garanteze securitatea și confidențialitatea datelor prelucrate și să ia toate măsurile de precauție necesare pentru a preveni controlul acestora de către persoane neautorizate. În special, actorii din acest sector ar trebui să aibă în vedere adoptarea următoarelor măsuri:

- criptarea canalelor de comunicare utilizând un algoritm de ultimă generație;
- implementarea unui sistem de gestionare a cheilor de criptare unic pentru fiecare vehicul, nu pentru fiecare model;
- pentru stocarea la distanță, criptarea datelor utilizând algoritmi de ultimă generație;
- reînnoirea periodică a cheilor de criptare;
- protejarea cheilor de criptare împotriva oricărei divulgări;
- autentificarea dispozitivelor de recepționare a datelor;
- asigurarea integrității datelor (de exemplu, prin hashing);
- accesarea datelor cu caracter personal prin tehnici fiabile de autentificare a utilizatorului (parolă, certificat electronic etc.).

94. În ceea ce privește producătorii de vehicule, CEPD recomandă implementarea următoarelor măsuri de securitate:

- separarea funcțiilor esențiale ale vehiculului de cele care se bazează întotdeauna pe capacitățile de telecomunicații (de exemplu, „infotainment”);
- implementarea unor măsuri tehnice care să le permită producătorilor de vehicule să corecteze rapid vulnerabilitățile în materie de securitate pe întreaga durată de viață a vehiculului;
- pentru funcțiile esențiale ale vehiculului, utilizarea cu prioritate, pe cât posibil, a unor mijloace de comunicare sigure, destinate în mod specific domeniului transporturilor;

- implementarea unui sistem de alarmă în cazul unui atac asupra sistemelor vehiculului, cu posibilitatea de a funcționa în regim de avarie[47];
- stocarea unui istoric al oricărui acces la sistemul de informații al vehiculului, de exemplu, cu până la șase luni în urmă, pentru a permite înțelegerea originii eventualelor atacuri și efectuarea periodică a unei revizuiri a informațiilor înregistrate pentru a detecta posibilele anomalii.

95. Aceste recomandări generale ar trebui completate de cerințe specifice, care iau în considerare caracteristicile și scopul fiecărei prelucrări de date cu caracter personal.

2.8 Transmiterea datelor cu caracter personal către terți

96. În principiu, doar operatorul și persoana vizată au acces la datele generate de un vehicul conectat. Cu toate acestea, operatorul poate transmite date cu caracter personal unui partener comercial (destinatar), în măsura în care acest transfer se bazează în mod legal pe unul dintre temeiurile juridice menționate la articolul 6 din RGPD.

97. Având în vedere posibila sensibilitate a datelor privind utilizarea vehiculului (de exemplu, călătorii efectuate, stilul de conducere), CEPD recomandă obținerea sistematică a consimțământului persoanei vizate înainte de transmiterea datelor acesteia unui partener comercial care acționează în calitate de operator de date (de exemplu, prin bifarea unei căsuțe care nu este bifată în prealabil sau, dacă este posibil din punct de vedere tehnic, prin utilizarea unui dispozitiv fizic sau logic pe care persoana în cauză îl poate accesa din vehicul). La rândul său, partenerul comercial devine responsabil pentru datele pe care le primește și trebuie să respecte toate dispozițiile RGPD.

98. Producătorul de vehicule, furnizorul de servicii sau un alt operator de date poate transmite date cu caracter personal către o persoană împuternicită de operator care are un rol în furnizarea serviciului către persoana vizată, cu condiția ca persoana împuternicită de operator să nu utilizeze datele respective în scopuri proprii. Operatorii și persoanele împuternicite de operatori încheie un contract sau un alt act juridic care menționează obligațiile fiecărei părți și include dispozițiile articolului 28 din RGPD.

2.9 Transferul de date cu caracter personal în afara UE/SEE

99. În cazul transferului de date cu caracter personal în afara Spațiului Economic European, sunt prevăzute garanții speciale pentru asigurarea protecției datelor.

100. În consecință, operatorul poate transfera date cu caracter personal unui destinatar numai în măsura în care acest transfer respectă cerințele prevăzute în capitolul V din RGPD.

[47] Regimul de avarie este un mod de funcționare a vehiculului care garantează menținerea funcțiilor esențiale pentru utilizarea în siguranță a acestuia (și anume, cerințele minime de siguranță), chiar dacă alte funcționalități mai puțin importante ar fi dezactivate (de exemplu, funcționarea dispozitivului de geoghidare poate fi considerată ca fiind neesențială, spre deosebire de sistemul de frânare).

2.10 Utilizarea tehnologiilor Wi-Fi încorporate la bordul vehiculelor

101. Progresele realizate în tehnologia celulară au făcut posibilă utilizarea cu ușurință a internetului în timpul deplasării cu vehiculul. Deși conectivitatea Wi-Fi într-un vehicul poate fi asigurată prin utilizarea unui smartphone ca punct de acces sau a unui dispozitiv dedicat (cheie OBD-II, modem sau router fără fir etc.), majoritatea producătorilor oferă în prezent modele cu o conexiune de date de rețea celulară integrată și care sunt, de asemenea, capabile să creeze rețele Wi-Fi. În funcție de caz, trebuie luate în considerare diverse aspecte:

- Conectivitatea Wi-Fi este oferită ca serviciu de un profesionist în domeniul transportului rutier, cum ar fi un șofer de taxi pentru clienții săi. În acest caz, profesionistul sau societatea pe care o reprezintă poate fi considerat(ă) un furnizor de servicii de internet (ISP) și, în consecință, poate face obiectul unor obligații și restricții specifice în ceea ce privește prelucrarea datelor cu caracter personal ale clienților.

- Conectivitatea Wi-Fi este destinată utilizării exclusive de către conducătorul auto (exclusiv pentru conducătorul auto și ocupanții vehiculului). În acest caz, prelucrarea datelor cu caracter personal este considerată a fi o activitate exclusiv personală sau domestică în conformitate cu articolul 2 alineatul (2) litera (c) și considerentul 18 din RGPD.

102. În general, conectarea tot mai frecventă la internet prin Wi-Fi prezintă riscuri mai ridicate pentru viața privată a persoanelor fizice. Într-adevăr, prin intermediul vehiculelor lor, utilizatorii devin emițători permanenți și, prin urmare, pot fi identificați și urmăriți. Pentru a preveni urmărirea, producătorii de vehicule și echipamente trebuie să pună în aplicare opțiuni de renunțare ușor de utilizat, care să împiedice colectarea identificatorului setului de servicii (SSID) al rețelei Wi-Fi încorporate la bord.

3 STUDII DE CAZ

103. În această secțiune sunt prezentate cinci exemple specifice de prelucrare a datelor cu caracter personal în contextul vehiculelor conectate, care corespund unor scenarii posibile pentru părțile interesate din acest sector. Exemplele se referă la prelucrarea datelor care necesită o putere de calcul ce nu poate fi mobilizată local în vehicul și/sau transferul de date cu caracter personal către un terț pentru efectuarea de analize suplimentare sau pentru furnizarea de funcționalități suplimentare de la distanță. Pentru fiecare tip de prelucrare, prezentul document specifică scopurile preconizate, categoriile de date colectate, perioada de păstrare a acestor date, drepturile persoanelor vizate, măsurile de securitate care trebuie puse în aplicare și destinatarii informațiilor. În cazul în care unele dintre aceste aspecte nu sunt descrise în paginile următoare, se aplică recomandările generale descrise în secțiunea anterioară.

104. Exemplele prezentate nu sunt exhaustive și au doar scopul de a indica varietatea tipurilor de prelucrare, a temeiurilor juridice, a actorilor implicați etc. în contextul vehiculelor conectate.

3.1 Furnizarea unui serviciu de către un terț

105. Persoanele vizate pot încheia contracte cu un furnizor de servicii pentru a beneficia de servicii cu valoare adăugată legate de utilizarea vehiculului. De exemplu, o persoană vizată poate încheia un contract de asigurare bazat pe utilizare, care oferă prime de asigurare reduse pentru deplasări mai puțin frecvente („plătești cât conduci”) sau un bun comportament la volan („plătești cum conduci”), și care necesită monitorizarea obiceiurilor de conducere de către societatea de asigurări. De asemenea, o persoană vizată poate să încheie un contract cu o societate care oferă asistență rutieră în caz de defecțiune

și care implică transmiterea datelor de localizare a vehiculului către societate sau cu un furnizor de servicii pentru a primi mesaje sau alerte referitoare la funcționarea vehiculului (de exemplu, o alertă cu privire la uzura frânelor sau o atenționare privind data următoarei inspecții tehnice).

3.1.1 Asigurare bazată de utilizare

106. „Plătești cât conduci" este un tip de asigurare bazată pe utilizare care urmărește distanța parcursă și/sau obiceiurile de conducere ale conducătorilor auto, pentru a-i identifica și a-i recompensa pe cei care conduc prudent, oferindu-le prime de asigurare mai mici. Societatea de asigurări îi va solicita conducătorului auto să instaleze un serviciu telematic integrat, o aplicație mobilă sau să activeze un modul integrat din fabrică care monitorizează distanța parcursă și/sau stilul de conducere (tipar de frânare, accelerare rapidă etc.) al titularului poliței de asigurare. Informațiile colectate de dispozitivul telematic vor fi utilizate pentru a atribui punctaje conducătorului auto în vederea analizării riscurilor pe care acesta le poate prezenta pentru societatea de asigurări.

107. Întrucât o asigurare bazată pe utilizare necesită exprimarea consimțământului de către persoana vizată în temeiul articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice, CEPD subliniază faptul că titularul poliței trebuie să aibă opțiunea de a alege o poliță de asigurare care nu se bazează pe utilizare. În caz contrar, consimțământul nu ar fi considerat ca fiind exprimat în mod liber, întrucât executarea contractului ar fi condiționată de acest consimțământ. În plus, articolul 7 alineatul (3) din RGPD prevede că o persoană vizată trebuie să aibă dreptul de a-și retrage în orice moment consimțământul.

3.1.1.1 Temei juridic

108. Atunci când datele sunt colectate prin intermediul unui serviciu public de comunicații electronice (de exemplu, prin intermediul cartelei SIM din dispozitivul telematic), consimțământul este necesar pentru a obține acces la informațiile deja stocate în vehicul, astfel cum se prevede la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. Într-adevăr, niciuna din derogările prevăzute la articolul menționat nu se poate aplica în acest context: prelucrarea nu este efectuată cu unicul scop de a efectua transmisia comunicației printr-o rețea de comunicații electronice și nici nu se referă la un serviciu al societății informaționale cerut în mod explicit de către abonat sau utilizator. Consimțământul ar putea fi obținut în momentul încheierii contractului.

109. În ceea ce privește prelucrarea datelor cu caracter personal în urma stocării sau a accesului la echipamentul terminal al utilizatorului final, societatea de asigurări se poate baza pe articolul 6 alineatul (1) litera (b) din RGPD în acest context specific, cu condiția să poată stabili că prelucrarea este efectuată în contextul unui contract valabil încheiat cu persoana vizată și că este necesară pentru executarea respectivului contract cu persoana vizată. În măsura în care prelucrarea este necesară în mod obiectiv pentru executarea contractului cu persoana vizată, CEPD consideră că invocarea articolului 6 alineatul (1) litera (b) din RGPD nu ar reduce protecția suplimentară prevăzută la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice în acest caz specific. Acest temei juridic se materializează prin semnarea de către persoana vizată a unui contract cu societatea de asigurări.

3.1.1.2 Datele colectate

110. Trebuie avute în vedere două tipuri de date cu caracter personal:

- **date comerciale și privind tranzacțiile**: datele de identificare ale persoanei vizate, datele referitoare la tranzacții, datele privind mijloacele de plată etc.;
- **date privind utilizarea**: datele cu caracter personal generate de vehicul, obiceiurile de conducere, datele de localizare etc.

111. CEPD recomandă ca, pe cât posibil și având în vedere riscul ca datele colectate prin intermediul dispozitivului telematic să fie utilizate în mod abuziv pentru a crea un profil precis al mișcărilor conducătorului auto, datele brute privind comportamentul la volan să fie prelucrate fie:

- în interiorul vehiculului, în dispozitivele telematice sau pe smartphone-ul utilizatorului, astfel încât societatea de asigurări să acceseze numai datele privind rezultatele (de exemplu, un punctaj referitor la obiceiurile de conducere), nu și datele brute detaliate (a se vedea secțiunea 2.1);

- sau de către furnizorul de servicii telematice în numele operatorului (societatea de asigurări), pentru a genera punctaje numerice care sunt transferate societății de asigurări la intervale stabilite. În acest caz, datele brute trebuie să fie separate de datele direct legate de identitatea conducătorului auto. Aceasta înseamnă că furnizorul de servicii telematice primește datele în timp real, dar nu cunoaște numele, numerele de înmatriculare etc. ale titularilor polițelor de asigurare. Pe de altă parte, societatea de asigurări cunoaște numele titularilor polițelor de asigurare, însă primește doar punctajele și numărul total de kilometri parcurși, nu și datele brute utilizate pentru a calcula aceste punctaje.

112. În plus, trebuie menționat faptul că, în cazul în care pentru executarea contractului este necesară doar informația legată de kilometraj, datele de localizare nu se colectează.

3.1.1.3 Perioada de păstrare

113. În contextul prelucrării datelor cu caracter personal pentru executarea unui contract (și anume, furnizarea unui serviciu), este important să se facă distincția între două tipuri de date înainte de a defini perioadele de păstrare respective:

- **date comerciale și privind tranzacțiile:** aceste date pot fi păstrate într-o bază de date activă pe întreaga durată a contractului. La sfârșitul contractului, acestea pot fi arhivate fizic (pe un suport separat: DVD etc.) sau logic (prin gestionarea autorizațiilor) în eventualitatea unui litigiu. Ulterior, la expirarea termenelor de prescripție legale, datele sunt șterse sau anonimizate;

- **date privind utilizarea:** datele privind utilizarea pot fi clasificate ca date brute și date agregate. Astfel cum s-a menționat mai sus, dacă este posibil, operatorii sau persoanele împuternicite de operatori nu ar trebui să prelucreze date brute. Dacă acest lucru este însă necesar, datele brute ar trebui să fie păstrate numai pe perioada necesară pentru elaborarea datelor agregate și pentru verificarea validității procesului de agregare respectiv. Datele agregate ar trebui să fie păstrate atât timp cât este necesar pentru furnizarea serviciului sau pe o perioadă prevăzută în dreptul Uniunii sau dreptul intern.

3.1.1.4 Informarea și drepturile persoanelor vizate

114. Înainte de prelucrarea datelor cu caracter personal, persoana vizată este informată, în conformitate cu articolul 13 din RGPD, într-un mod transparent și inteligibil. În special, persoana vizată trebuie să fie informată cu privire la perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, cu privire la criteriile utilizate pentru stabilirea acestei perioade. În acest ultim caz, CEPD recomandă adoptarea unei abordări pedagogice pentru a sublinia diferența dintre datele brute și punctajul obținut pe baza acestora, evidențiind, atunci când este cazul, faptul că societatea de asigurări va colecta datele pe baza cărora a fost obținut punctajul doar dacă este cazul.

115. Atunci când datele nu sunt prelucrate în interiorul vehiculului, ci de către un furnizor de servicii telematice în numele operatorului (societatea de asigurări), ar fi util ca persoana vizată să fie informată că, în acest caz, furnizorul nu va avea acces la date direct legate de identitatea conducătorului auto (cum ar fi numele, numărul de înmatriculare etc.). De asemenea, având în vedere importanța informării persoanelor vizate cu privire la

consecințele prelucrării datelor cu caracter personal care le privesc și faptul că persoanele vizate nu ar trebui să fie luate prin surprindere de o astfel de prelucrare, CEPD recomandă ca persoana vizată să fie informată cu privire la crearea de profiluri și la consecințele creării de profiluri, chiar dacă aceasta nu implică niciun proces decizional automatizat, astfel cum se menționează la articolul 22 din RGPD.

116. În ceea ce privește drepturile persoanelor vizate, acestea sunt informate în mod specific cu privire la mijloacele disponibile pentru a-și exercita dreptul de acces, rectificare și ștergere a datelor, precum și de restricționare a prelucrării. Întrucât datele brute colectate în acest context sunt furnizate de persoana vizată (prin formulare specifice sau prin activitatea acesteia) și prelucrate în temeiul articolului 6 alineatul (1) litera (b) din RGPD (executarea unui contract), persoana vizată are dreptul să își exercite dreptul la portabilitatea datelor. Astfel cum se subliniază în orientările privind dreptul la portabilitatea datelor, CEPD recomandă cu fermitate „ca operatorii de date să explice în mod clar diferența între tipurile de date pe care o persoană vizată le poate primi ca urmare a exercitării dreptului de acces și a dreptului la portabilitatea datelor”[48].

117. Informațiile pot fi furnizate în momentul semnării contractului.

3.1.1.5 Destinatar:

118. CEPD recomandă ca, pe cât posibil, datele privind utilizarea vehiculului să fie prelucrate direct în dispozitivele telematice, astfel încât societatea de asigurări să acceseze doar datele privind rezultatele (de exemplu, un punctaj), nu și date brute detaliate.

119. Atunci când un furnizor de servicii telematice colectează datele în numele operatorului (societatea de asigurări) pentru a genera punctaje numerice, nu este nevoie ca acesta să cunoască identitatea conducătorului auto (precum numele, numerele de înmatriculare etc.) în ceea ce privește titularii polițelor de asigurare.

3.1.1.6 Securitate:

120. Se aplică recomandările generale. A se vedea secțiunea 2.7.

3.1.2 Închirierea și rezervarea unui loc de parcare

121. În cazul în care proprietarul unui loc de parcare dorește să îl închirieze, stabilește un preț și încarcă datele privind locul de parcare respectiv într-o aplicație web. Apoi, aplicația îi transmite notificări proprietarului atunci când un conducător auto dorește să îl rezerve. Conducătorul auto poate selecta o destinație și poate căuta locuri de parcare disponibile pe baza mai multor criterii. După aprobarea proprietarului, tranzacția este confirmată și furnizorul de servicii gestionează operațiunea de plată, apoi conducătorul auto utilizează sistemul de navigație pentru a ajunge la locul respectiv.

3.1.2.1 Temei juridic

122. Atunci când datele sunt colectate prin intermediul unui serviciu public de comunicații electronice, se aplică dispozițiile articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.

123. Întrucât este vorba despre un serviciu al societății informaționale, articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice nu impune obținerea consimțământului pentru accesarea informațiilor deja stocate în vehicul atunci când acest serviciu este cerut în mod explicit de către abonat.

[48] Grupul de lucru „Articolul 29”, Orientări privind dreptul la portabilitatea datelor în temeiul Regulamentului 2016/676, WP242 rev.01, aprobate de CEPD, p. 13.

124. Articolul 6 alineatul (1) litera (b) din RGPD va constitui temeiul juridic pentru prelucrarea datelor cu caracter personal și numai pentru datele necesare pentru executarea contractului la care persoana vizată este parte.

3.1.2.2 Datele colectate

125. Datele prelucrate includ datele de contact ale conducătorului auto [numele, adresa de e-mail, numărul de telefon, tipul de vehicul (de exemplu, autoturism, camion, motocicletă), numărul de înmatriculare, perioada de staționare, detaliile plății (de exemplu, informații privind cardul de credit), precum și datele de navigație.

3.1.2.3 Perioada de păstrare

126. Datele trebuie să fie păstrate numai pe perioada necesară pentru executarea contractului de parcare sau după cum se prevede în dreptul Uniunii sau dreptul intern. După expirarea acestei perioade, datele sunt anonimizate sau șterse.

3.1.2.4 Informarea și drepturile persoanelor vizate

127. Înainte de prelucrarea datelor cu caracter personal, persoana vizată ar trebui să fie informată, în conformitate cu articolul 13 din RGPD, într-un mod transparent și inteligibil.

128. Persoana vizată ar trebui să fie informată în mod specific cu privire la mijloacele disponibile pentru a-și exercita dreptul de acces, rectificare și ștergere a datelor, precum și de restricționare a prelucrării. Întrucât datele colectate în acest context sunt furnizate de persoana vizată (prin formulare specifice sau prin activitatea acesteia) și prelucrate în temeiul articolului 6 alineatul (1) litera (b) din RGPD (executarea unui contract), persoana vizată are dreptul de a-și exercita dreptul la portabilitatea datelor. Astfel cum se subliniază în Orientările privind dreptul la portabilitatea datelor, CEPD recomandă cu fermitate „ca operatorii de date să explice în mod clar diferența între tipurile de date pe care o persoană vizată le poate primi ca urmare a exercitării dreptului de acces și a dreptului la portabilitatea datelor”.

3.1.2.5 Destinatar*:*

129. În principiu, doar operatorul de date și persoana împuternicită de operator au acces la date.

3.1.2.6 Securitate:

130. Se aplică recomandările generale. A se vedea secțiunea 2.7.

3.2 eCall

131. În cazul unui accident grav produs în Uniunea Europeană, vehiculul inițiază automat un apel de urgență la 112, numărul de urgență valabil la nivelul UE (a se vedea secțiunea 1.1 pentru detalii suplimentare), care permite trimiterea rapidă a unei ambulanțe la locul accidentului, în conformitate cu Regulamentul (UE) 2015/758 din 29 aprilie 2015 privind cerințele de omologare de tip pentru instalarea sistemului eCall bazat pe serviciul 112 la bordul vehiculelor și de modificare a Directivei 2007/46/CE [denumit în continuare „Regulamentul (UE) 2015/758”].

132. Într-adevăr, sistemul eCall instalat în vehicul, care permite transmisia prin intermediul unei rețele publice de comunicații mobile fără fir, inițiază un apel de urgență, care este efectuat fie automat, prin activarea unor senzori de la bordul vehiculului, fie manual de către ocupanții acestuia numai în cazul unui accident. Pe lângă activarea canalului audio, al doilea eveniment care are loc automat în urma producerii unui accident constă în generarea setului minim de date (MSD) și transmiterea acestuia către centrul de preluare a apelurilor de urgență (PSAP).

3.2.1 Temei juridic

133. În ceea ce privește aplicarea Directivei privind viața privată și comunicațiile electronice, trebuie avute în vedere două dispoziții:

- articolul 9 privind datele de localizare, altele decât datele de transfer, care se aplică exclusiv serviciilor de comunicații electronice;
- articolul 5 alineatul (3) pentru obținerea accesului la informațiile stocate în sistemul instalat în vehicul.

134. În pofida faptului că, în principiu, aceste dispoziții prevăd consimțământul persoanei vizate, Regulamentul (UE) 2015/758 constituie o obligație legală care îi revine operatorului de date (persoana vizată nu dispune cu adevărat de libertatea de alegere și nu va fi în măsură să refuze prelucrarea datelor care o privesc). Prin urmare, Regulamentul (UE) 2015/758 prevalează asupra obligației de obținere a consimțământului din partea conducătorului auto pentru prelucrarea datelor de localizare și a setului minim de date[49].

135. Temeiul juridic al prelucrării datelor respective va fi îndeplinirea unei obligații legale, astfel cum se prevede la articolul 6 alineatul (1) litera (c) din RGPD [și anume, Regulamentul (UE) 2015/758].

3.2.2 Datele colectate

136. Regulamentul (UE) 2015/758 prevede că datele trimise de sistemul eCall bazat pe serviciul 112 instalat la bordul vehiculului includ doar informațiile minime definite de standardul EN 15722:2015 „Sisteme de transport inteligente – eSafety – Setul minim de date eCall”, inclusiv:

- indicarea inițierii manuale sau automate a apelului de urgență;
- tipul de vehicul;
- numărul de identificare al vehiculului (VIN);
- tipul de sistem de propulsie al vehiculului;
- marcajul temporal pentru generarea inițială a mesajului de date în cadrul evenimentului eCall actual;
- ultimele coordonate de latitudine și longitudine cunoscute, determinate cât mai aproape posibil de momentul generării mesajului;
- ultima direcție de deplasare efectivă cunoscută a vehiculului, determinată cât mai aproape posibil de momentul generării mesajului (doar ultimele trei localizări ale vehiculului).

3.2.3 Perioada de păstrare

137. Regulamentul (UE) 2015/758 prevede că datele nu se păstrează mai mult decât este necesar în scopul gestionării situațiilor de urgență. Astfel de date se elimină în totalitate de îndată ce nu mai sunt necesare în acest scop. În plus, datele din memoria internă a sistemului eCall sunt eliminate în mod automat și în mod continuu. Se permite păstrarea numai a ultimelor trei localizări ale vehiculului, în măsura în care acest lucru este strict necesar pentru a preciza situarea actuală și direcția de deplasare la momentul evenimentului.

[49] Trebuie menționat faptul că articolul 8 alineatul (1) litera (f) din mandatul de negociere al Consiliului pentru propunerea de regulament privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice prevede o derogare specifică pentru eCall, consimțământul nefiind necesar „dacă acest lucru este necesar pentru a localiza echipamentul terminal atunci când un utilizator final efectuează o comunicare de urgență fie cu numărul european unic pentru apeluri de urgență «112», fie cu un număr național pentru apeluri de urgență, în conformitate cu articolul 13 alineatul (3)”.

3.2.4 Informarea și drepturile persoanelor vizate

138. Articolul 6 din Regulamentul (UE) 2015/758 prevede obligația producătorilor de a furniza informații clare și complete cu privire la activitățile de prelucrare a datelor efectuate prin intermediul sistemului eCall. Aceste informații sunt furnizate în manualul utilizatorului în mod separat pentru sistemul eCall bazat pe serviciul 112 instalat la bordul autovehiculului și pentru sistemele eCall asigurate de terți, înainte de utilizarea sistemului. Acestea includ:

- trimiterea la temeiul juridic al prelucrării;
- faptul că sistemul eCall bazat pe serviciul 112 instalat la bordul vehiculului este activat implicit;
- modalitățile de prelucrare a datelor pe care o efectuează sistemul eCall bazat pe serviciul 112 instalat la bordul vehiculului;
- scopul specific al prelucrării apelurilor eCall, care este limitat la situațiile de urgență menționate la articolul 5 alineatul (2) primul paragraf din Regulamentul (UE) 2015/758;
- tipurile de date colectate și prelucrate și destinatarii acestor date;
- termenul pentru păstrarea datelor în sistemul eCall bazat pe serviciul 112 instalat la bordul autovehiculului;
- faptul că nu există o monitorizare constantă a vehiculului;
- modalitățile pentru exercitarea drepturilor persoanelor vizate, precum și serviciul de contact responsabil de gestionarea cererilor de acces;
- orice informație suplimentară necesară în ceea ce privește urmărirea, detectarea și prelucrarea datelor cu caracter personal în legătură cu furnizarea unui serviciu eCall de către prestatori terți (TPS) și/sau a altor servicii cu valoare adăugată, care face obiectul consimțământului explicit al proprietarului și este în conformitate cu RGPD. Se ține seama în mod special de diferențele ce se pot înregistra între prelucrarea datelor prin intermediul sistemului eCall bazat pe serviciul 112 instalat la bordul autovehiculului și sistemele eCall asigurate de terți sau alte servicii cu valoare adăugată.

139. De asemenea, furnizorul de servicii transmite persoanelor vizate informațiile specificate la articolul 13 din RGPD, într-un mod transparent și inteligibil. În special, persoana vizată trebuie să fie informată cu privire la scopurile prelucrării pentru care au fost colectate datele cu caracter personal, precum și cu privire la faptul că prelucrarea acestor date se bazează pe o obligație legală care îi revine operatorului.

140. În plus, ținând cont de natura prelucrării, informațiile cu privire la destinatarii sau categoriile de destinatari ai datelor cu caracter personal ar trebui să fie clare, iar persoanele vizate ar trebui să fie informate că datele nu sunt disponibile în afara sistemului eCall bazat pe serviciul 112 instalat la bordul vehiculului pentru nicio entitate înainte de declanșarea apelului eCall.

141. În ceea ce privește drepturile persoanelor vizate, trebuie menționat faptul că, întrucât prelucrarea are ca temei o obligație legală, dreptul la opoziție și dreptul la portabilitatea datelor nu se aplică.

3.2.5 Destinatar:

142. Datele nu sunt disponibile în afara sistemului eCall bazat pe serviciul 112 instalat la bordul vehiculului pentru nicio entitate înainte de declanșarea apelului eCall.

143. Atunci când este activat (fie manual de către ocupanții vehiculului, fie automat imediat ce un senzor montat pe vehicul detectează o coliziune gravă), sistemul eCall stabilește o conexiune vocală cu PSAP relevant, iar setul minim de date este trimis operatorului PSAP.

144. În plus, datele transmise prin intermediul sistemului eCall bazat pe serviciul 112 instalat la bordul vehiculului și prelucrate de PSAP-uri pot fi transferate serviciului de urgență și partenerilor din serviciu menționați în Decizia nr. 585/2014/UE doar în cazul unor incidente legate de apelurile eCall și sub rezerva condițiilor specificate de respectiva decizie și sunt utilizate exclusiv în scopul atingerii obiectivelor respectivei decizii. Datele prelucrate de PSAP-uri prin intermediul sistemului eCall bazat pe serviciul 112 instalat la bordul vehiculului nu sunt transferate niciunei părți terțe fără acordul prealabil explicit al persoanei vizate.

3.2.6 Securitate

145. Regulamentul (UE) 2015/758 prevede cerința de a integra în sistemul eCall tehnologii de consolidare a protecției vieții private pentru a oferi utilizatorilor nivelul adecvat de protecție a vieții private, precum și garanțiile necesare pentru prevenirea supravegherii persoanelor fizice și utilizării abuzive a datelor. În plus, producătorii garantează că sistemul eCall bazat pe serviciul 112 instalat la bordul vehiculului și orice sistem suplimentar care oferă un apel eCall asigurat de terți sau un serviciu cu valoare adăugată sunt concepute astfel încât între acestea să nu fie posibil niciun schimb de date cu caracter personal.

146. Referitor la PSAP-uri, statele membre se asigură că datele cu caracter personal sunt protejate împotriva utilizării abuzive, inclusiv împotriva accesului neautorizat, a modificării sau a pierderii și că protocoalele privind stocarea, perioada de păstrare, prelucrarea și protecția datelor cu caracter personal sunt stabilite la nivelul corespunzător și sunt respectate în mod corespunzător.

3.3 Studii de accidentologie

147. Persoanele vizate pot participa în mod voluntar la studii de accidentologie realizate pentru a înțelege mai bine cauzele accidentelor rutiere și, la un nivel mai general, în scopuri științifice.

3.3.1 Temei juridic

148. Atunci când datele sunt colectate prin intermediul unui serviciu public de comunicații electronice, operatorul de date trebuie să obțină consimțământul persoanei vizate pentru accesarea informațiilor deja stocate în vehicul, astfel cum se prevede la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice. Într-adevăr, niciuna din derogările prevăzute la articolul menționat nu se poate aplica în acest context: prelucrarea nu este efectuată cu unicul scop de a efectua transmisia comunicației printr-o rețea de comunicații electronice și nici nu se referă la un serviciu al societății informaționale cerut în mod explicit de către abonat sau utilizator.

149. În ceea ce privește prelucrarea datelor cu caracter personal și ținând cont de varietatea și volumul de date cu caracter personal necesare pentru studiile de accidentologie, CEPD recomandă ca prelucrarea să se bazeze pe consimțământul prealabil al persoanei vizate, în conformitate cu articolul 6 din RGPD. Acest consimțământ prealabil trebuie exprimat într-un formular specific, prin care persoana vizată este de acord să participe în mod voluntar la studiu și ca datele cu caracter personal care o privesc să fie prelucrate în acest scop. Consimțământul este o manifestare a voinței liber exprimate, specifice și în cunoștință de cauză a persoanei ale cărei date sunt prelucrate (de exemplu, bifarea unei căsuțe care nu este bifată în prealabil sau configurarea computerului de bord pentru a activa o funcție în vehicul). Consimțământul trebuie să fie acordat separat, pentru scopuri specifice, nu poate fi asociat executării contractului de vânzare-cumpărare sau de leasing al unui automobil nou și trebuie să poată fi retras cu aceeași ușurință cu care a fost acordat. Retragerea consimțământului are ca efect încetarea prelucrării. Datele sunt apoi șterse din baza de date activă sau anonimizate.

150. Consimțământul prevăzut la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice și cel necesar ca temei juridic pentru prelucrarea datelor pot fi obținute în același timp (de exemplu, prin bifarea unei căsuțe care indică în mod clar pentru ce își exprimă consimțământul persoana vizată).

151. Trebuie menționat faptul că, în funcție de condițiile prelucrării (natura operatorului de date etc.), un alt temei juridic poate fi invocat în mod legal atât timp cât nu reduce protecția suplimentară prevăzută la articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice (a se vedea punctul 15). În cazul în care prelucrarea se bazează pe un alt temei juridic, cum ar fi îndeplinirea unei sarcini care servește unui interes public [articolul 6 alineatul (1) litera (e) din RGPD], CEPD recomandă ca persoanele vizate să fie incluse în studiu în mod voluntar.

3.3.2 Datele colectate

152. Operatorul colectează doar datele cu caracter personal care sunt strict necesare pentru scopul prelucrării.

153. Două tipuri de date trebuie luate în considerare:

- **date referitoare la participanți și la vehicule**;
- **date tehnice provenite de la vehicule** (viteza instantanee etc.).

154. Cercetarea științifică legată de accidentologie justifică colectarea informației privind viteza instantanee, inclusiv de către persoanele juridice care nu administrează un serviciu public în sens strict.

155. Într-adevăr, astfel cum s-a menționat mai sus, CEPD consideră că viteza instantanee colectată în contextul unui studiu de accidentologie nu reprezintă date privind infracțiunile propriu-zis (și anume, nu sunt colectate în scopul cercetării sau urmăririi penale a unei infracțiuni), ceea ce justifică colectarea acesteia de către persoane juridice care nu administrează un serviciu public în sens strict.

3.3.3 Perioada de păstrare

156. Este important să se facă distincția între două tipuri de date. În primul rând, datele referitoare la participanți și la vehicule pot fi păstrate pe durata studiului. În al doilea rând, datele tehnice provenite de la vehicule ar trebui păstrate pentru o perioadă care nu depășește perioada necesară îndeplinirii scopului în care au fost colectate. Cinci ani de la data încheierii studiului pare a fi o perioadă rezonabilă în acest sens. La sfârșitul perioadei respective, datele sunt șterse sau anonimizate.

3.3.4 Informarea și drepturile persoanelor vizate

157. Înainte de prelucrarea datelor cu caracter personal, persoana vizată este informată, în conformitate cu articolul 13 din RGPD, într-un mod transparent și inteligibil. În special, în cazul colectării informației privind viteza instantanee, persoanele vizate ar trebui să fie informate în mod specific cu privire la colectarea acestor date. Întrucât prelucrarea datelor se bazează pe consimțământ, persoana vizată trebuie să fie informată în mod specific cu privire la existența dreptului de a-și retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. În plus, deoarece datele colectate în acest context sunt furnizate de persoana vizată (prin formulare specifice sau prin activitatea acesteia) și prelucrate în temeiul articolului 6 alineatul (1) litera (a) din RGPD (consimțământ), persoana vizată își poate exercita dreptul la portabilitatea datelor. Astfel cum se subliniază în Orientările privind dreptul la portabilitatea datelor, CEPD recomandă cu fermitate „ca operatorii de date să explice în mod clar diferența între tipurile de date pe care o persoană vizată le poate primi ca urmare a exercitării dreptului de acces și a dreptului la portabilitatea datelor”. În consecință,

operatorul ar trebui să ofere persoanei vizate o modalitate ușoară de a-și retrage consimțământul, în mod liber și în orice moment, și să dezvolte instrumente pentru a putea răspunde cererilor de portabilitate a datelor.

158. Aceste informații pot fi furnizate la semnarea formularului de consimțământ pentru participarea la studiul de accidentologie.

3.3.5 Destinatar

159. În principiu, doar operatorul de date și persoana împuternicită de operator au acces la date.

3.3.6 Securitate

160. După cum s-a menționat mai sus, măsurile de securitate instituite sunt adaptate la nivelul de sensibilitate a datelor. De exemplu, în cazul în care viteza instantanee (sau orice alte date referitoare la condamnări penale și infracțiuni) este colectată în cadrul studiului de accidentologie, CEPD recomandă cu fermitate instituirea unor măsuri de securitate solide, cum ar fi:

- punerea în aplicare a unor măsuri de pseudonimizare (de exemplu, hashing cu cheie secretă pentru date precum numele/prenumele persoanei vizate și numărul secvențial);
- stocarea datelor privind viteza instantanee și de localizare în baze de date separate (de exemplu, utilizând un mecanism de criptare de ultimă generație cu chei și mecanisme de aprobare distincte);
- și/sau ștergerea datelor de localizare imediat după stabilirea evenimentului sau a secvenței de referință (de exemplu, tipul de drum, zi/noapte) și stocarea datelor de identificare directă într-o bază de date separată care poate fi accesată doar de un număr restrâns de persoane.

3.4 Furtul vehiculului

161. În caz de furt, persoanele vizate pot dori să încerce să își găsească vehiculul pe baza datelor de localizare. Utilizarea datelor de localizare se limitează la nevoile stricte ale investigației și la evaluarea cazului de către autoritățile judiciare competente.

3.4.1 Temei juridic

162. Atunci când datele sunt colectate prin intermediul unui serviciu public de comunicații electronice, se aplică dispozițiile articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.

163. Întrucât este vorba despre un serviciu al societății informaționale, articolul 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice nu impune obținerea consimțământului pentru accesarea informațiilor deja stocate în vehicul atunci când acest serviciu este cerut în mod explicit de către abonat.

164. În ceea ce privește prelucrarea datelor cu caracter personal, temeiul juridic pentru prelucrarea datelor de localizare va fi consimțământul proprietarului vehiculului sau, dacă este cazul, executarea unui contract (numai pentru datele necesare pentru executarea contractului la care proprietarul vehiculului este parte).

165. Consimțământul este o manifestare a voinței liber exprimate, specifice și în cunoștință de cauză a persoanei ale cărei date sunt prelucrate (de exemplu, bifarea unei căsuțe care nu este bifată în prealabil sau configurarea computerului de bord pentru a activa o funcție în vehicul). Libertatea de exprimare a consimțământului implică posibilitatea de retragere a acestuia în orice moment, iar persoana vizată ar trebui informată în mod expres în acest sens. Retragerea consimțământului are ca efect încetarea prelucrării. Datele ar trebui apoi șterse din baza de date activă, anonimizate sau arhivate.

3.4.2 Datele colectate

166. Datele de localizare pot fi transmise numai începând cu data raportării furtului și nu pot fi colectate în mod continuu în restul timpului.

3.4.3 Perioada de păstrare

167. Datele de localizare pot fi păstrate numai pentru perioada în care cazul este investigat de autoritățile judiciare competente sau până la încheierea unei proceduri de înlăturare a îndoielilor care nu se încheie odată cu confirmarea furtului vehiculului.

3.4.4 Informații pentru persoanele vizate

168. Înainte de prelucrarea datelor cu caracter personal, persoana vizată ar trebui să fie informată, în conformitate cu articolul 13 din RGPD, într-un mod transparent și inteligibil. Mai precis, CEPD recomandă ca operatorul de date să sublinieze faptul că nu are loc o monitorizare constantă a vehiculului și că datele de localizare pot fi colectate și transmise doar începând cu data raportării furtului. În plus, operatorul trebuie să furnizeze persoanei vizate informații referitoare la faptul că numai agenții autorizați ai platformei de supraveghere la distanță și autoritățile competente potrivit legii au acces la aceste date.

169. În ceea ce privește drepturile persoanelor vizate, atunci când prelucrarea datelor se bazează pe consimțământ, persoana vizată ar trebui să fie informată în mod specific cu privire la existența dreptului de a-și retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. În plus, atunci când datele colectate în acest context sunt furnizate de persoana vizată (prin formulare specifice sau prin activitatea acesteia) și prelucrate în temeiul articolului 6 alineatul (1) litera (a) (consimțământ) sau al articolului 6 alineatul (1) litera (b) din RGPD (executarea unui contract), persoana vizată își poate exercita dreptul la portabilitatea datelor. Astfel cum se subliniază în Orientările privind dreptul la portabilitatea datelor, CEPD recomandă cu fermitate „ca operatorii de date să explice în mod clar diferența între tipurile de date pe care o persoană vizată le poate primi ca urmare a exercitării dreptului de acces și a dreptului la portabilitatea datelor”.

170. În consecință, operatorul ar trebui să ofere persoanei vizate o modalitate ușoară de a-și retrage consimțământul (numai atunci când consimțământul constituie temeiul juridic), în mod liber și în orice moment, și să dezvolte instrumente pentru a putea răspunde cererilor de portabilitate a datelor.

171. Informațiile pot fi furnizate în momentul semnării contractului.

3.4.5 Destinatari

172. În cazul raportării unui furt, datele de localizare pot fi transmise (i) agenților autorizați ai platformei de supraveghere la distanță și (ii) autorităților competente potrivit legii.

3.4.6 Securitate

173. Se aplică recomandările generale. A se vedea secțiunea 2.7