Wytyczne 01/2020 dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu i aplikacji związanych z mobilnością

Wersja 2.0

Przyjęto dnia 9 marca 2021 r.

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

Historia wersji

Wersja 2.0	9 marca 2021 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	28 stycznia 2020 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE

1. Samochód – symbol gospodarki XX wieku – jest jednym z masowych dóbr konsumpcyjnych, które mają wpływ na całe społeczeństwo. Powszechnie kojarzone z pojęciem wolności, samochody są często postrzegane jako coś więcej niż tylko środek transportu. Faktycznie stanowią one obszar prywatny, w którym ludzie mogą korzystać z pewnej formy autonomii w podejmowaniu decyzji, bez jakiejkolwiek ingerencji z zewnątrz. Obecnie, wraz z upowszechnianiem się pojazdów podłączonych do internetu, taka wizja nie odpowiada już rzeczywistości. Łączność w pojazdach szybko rozszerza się z modeli luksusowych i marek „premium" na masowo produkowane modele średniej klasy, a pojazdy stają się olbrzymimi centrami danych. Nie tylko pojazdy, lecz również kierowcy i pasażerowie są w coraz większym stopniu połączeni z internetem. Faktycznie wiele modeli wprowadzonych na rynek w ciągu ostatnich kilku lat posiada zintegrowane czujniki i podłączone do internetu urządzenia pokładowe, które mogą gromadzić i rejestrować dane, takie jak osiągi silnika, nawyki kierowcy, odwiedzone miejsca, a potencjalnie nawet ruchy oczu kierowcy, tętno kierowcy lub dane biometryczne w celu jednoznacznej identyfikacji danej osoby[2].

2. Takie przetwarzanie danych odbywa się w złożonym ekosystemie, który nie ogranicza się do tradycyjnych podmiotów przemysłu motoryzacyjnego, lecz kształtowany jest również przez pojawianie się nowych podmiotów z sektora gospodarki cyfrowej. Te nowe podmioty mogą oferować usługi informacyjno-rozrywkowe, takie jak muzyka online, informacje o warunkach i ruchu na drodze, lub zapewniać systemy i usługi wspomagania kierowcy, takie jak oprogramowanie autopilota, aktualne informacje o stanie pojazdu, ubezpieczenia oparte na użytkowaniu lub dynamiczne tworzenie map. Ponadto, ponieważ pojazdy są podłączone do internetu za pomocą sieci łączności elektronicznej, zarządcy infrastruktury drogowej i operatorzy telekomunikacyjni zaangażowani w ten proces również odgrywają ważną rolę w odniesieniu do potencjalnych operacji przetwarzania danych osobowych kierowców i pasażerów.

3. Co więcej, pojazdy podłączone do internetu generują coraz większe ilości danych, z których większość można uznać za dane osobowe, gdyż dotyczą kierowców lub pasażerów. Nawet jeśli dane zgromadzone przez samochód podłączony do internetu nie są bezpośrednio powiązane z nazwiskiem danej osoby, z technicznymi aspektami i funkcjami pojazdu, będą

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Infografika „Data and the connected car [Dane i samochód podłączony do internetu], Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

one dotyczyły kierowcy lub pasażerów samochodu. Przykładowo dane odnoszące się do stylu jazdy lub pokonanej odległości, dane związane z zużyciem części pojazdu, dane dotyczące lokalizacji lub dane gromadzone przez kamery mogą dotyczyć zachowania kierowcy, a także informacji o innych osobach, które mogą znajdować się w pojeździe lub przechodzić obok. Takie dane techniczne generuje osoba fizyczna i umożliwiają jej bezpośrednią lub pośrednią identyfikację przez administratora danych lub przez inną osobę. Pojazd może być traktowany jako terminal, z którego mogą korzystać różni użytkownicy. W związku z tym, podobnie jak w przypadku komputera osobistego, ta potencjalna mnogość użytkowników nie wpływa na osobowy charakter danych.

4. W 2016 r. Fédération Internationale de l'Automobile (FIA) przeprowadziła w Europie kampanię pod nazwą „Mój samochód – moje dane", aby uzyskać informacje na temat tego, co Europejczycy myślą o samochodach podłączonych do internetu[3]. Kampania uwidoczniła wprawdzie duże zainteresowanie kierowców kwestią łączności, lecz zwróciła również uwagę na czujność, jaką należy zachowywać w odniesieniu do wykorzystywania danych uzyskanych z pojazdów, a także znaczenie przestrzegania przepisów w zakresie ochrony danych osobowych. Wyzwanie polega zatem na tym, aby każda zainteresowana strona uwzględniła wymiar „ochrony danych osobowych" już na etapie projektowania produktu oraz zapewniła użytkownikom samochodów przejrzystość i kontrolę w zakresie ich danych zgodnie z motywem 78 RODO. Takie podejście pomaga zwiększyć zaufanie użytkowników, a tym samym przyczynia się do długoterminowego rozwoju tych technologii.

1.1 Powiązane prace

5. W ostatnim dziesięcioleciu pojazdy podłączone do internetu stały się istotnym tematem dla organów regulacyjnych, przy czym w ciągu kilku ostatnich lat poświęcono im o wiele więcej uwagi. W związku z tym na szczeblu krajowym i międzynarodowym opublikowano różne dokumenty na temat bezpieczeństwa i prywatności pojazdów podłączonych do internetu. Te uregulowania i inicjatywy mają na celu uzupełnienie istniejących ram ochrony danych i prywatności o przepisy szczegółowe dotyczące danego sektora lub zapewnienie wytycznych specjalistom.

1.1.1 Inicjatywy na szczeblu europejskim i inicjatywy międzynarodowe

6. Od dnia 31 marca 2018 r. system pokładowy eCall oparty na numerze 112 jest obowiązkowy we wszystkich nowych typach pojazdów kategorii M1 i N1 (samochodach osobowych i pojazdach lekkich)[4,5]. W 2006 r. Grupa Robocza Art. 29 przyjęła dokument roboczy w sprawie ochrony danych i wpływu na prywatność w kontekście inicjatywy eCall[6]. Ponadto, jak już wcześniej omówiono, Grupa Robocza Art. 29 przyjęła również w październiku 2017 r. opinię dotyczącą przetwarzania danych osobowych w kontekście współpracujących inteligentnych systemów transportowych (C-ITS).

7. W styczniu 2017 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opublikowała badanie dotyczące cyberbezpieczeństwa i odporności inteligentnych samochodów zawierające wykaz elementów wrażliwych wraz z odpowiadającymi im zagrożeniami, rodzajami ryzyka, czynnikami je łagodzącymi oraz możliwymi do wdrożenia środkami

[3] Kampania „Mój samochód – moje dane"; http://www.mycarmydata.eu/.
[4] Interoperacyjna usługa eCall na terenie całej UE; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decyzja Parlamentu Europejskiego i Rady nr 585/2014/UE z dnia 15 maja 2014 r. w sprawie wdrożenia interoperacyjnej usługi eCall na terenie całej UE, Tekst mający znaczenie dla EOG; https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014D0585.
[6] Dokument roboczy w sprawie ochrony danych i wpływu na prywatność w kontekście inicjatywy eCall; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_pl.pdf.

bezpieczeństwa[7]. We wrześniu 2017 r. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności przyjęła rezolucję w sprawie pojazdów podłączonych do internetu[8]. Ponadto w kwietniu 2018 r. Międzynarodowa Grupa Robocza ds. Ochrony Danych w Telekomunikacji również przyjęła dokument roboczy w sprawie pojazdów podłączonych do internetu[9].

1.1.2 Krajowe inicjatywy członków Europejskiej Rady Ochrony Danych (EROD)

8. W styczniu 2016 r. Konferencja Niemieckich Federalnych i Krajowych Organów Ochrony Danych oraz Niemieckie Stowarzyszenie Przemysłu Motoryzacyjnego (VDA) opublikowały wspólne oświadczenie w sprawie zasad ochrony danych w pojazdach podłączonych i niepodłączonych do internetu[10]. W sierpniu 2017 r. brytyjskie Centre for Connected and Autonomous Vehicles (CCAV) [Centrum ds. Pojazdów Podłączonych do Internetu i Pojazdów Autonomicznych] opublikowało przewodnik określający zasady cyberbezpieczeństwa dotyczące pojazdów podłączonych do internetu i pojazdów zautomatyzowanych w celu zwiększenia świadomości w tym kontekście w sektorze motoryzacyjnym[11]. W październiku 2017 r. francuski organ ochrony danych, Commission Nationale de l'Informatique et des Libertés (CNIL), opublikował pakiet środków zapewniających zgodność z przepisami w odniesieniu do samochodów podłączonych do internetu, aby pomóc zainteresowanym stronom w zakresie uwzględniania zasady ochrony danych już w fazie projektowania oraz zasady domyślnej ochrony danych, zapewniając osobom, których dane dotyczą, skuteczną kontrolę nad własnymi danymi osobowymi[12].

1.2 Prawo właściwe

9. Właściwe unijne ramy prawne w tym kontekście zapewnia RODO. Rozporządzenie ma zastosowanie w każdym przypadku, w którym przetwarzanie danych w kontekście pojazdów podłączonych do internetu wiąże się z przetwarzaniem danych osobowych osób fizycznych.

10. Oprócz przepisów RODO w dyrektywie 2002/58/WE zmienionej dyrektywą 2009/136/WE („dyrektywa o e-prywatności") **określono szczególną normę dla wszystkich podmiotów chcących przechowywać informacje w urządzeniu końcowym abonenta lub użytkownika na terenie Europejskiego Obszaru Gospodarczego (EOG) lub uzyskiwać dostęp do takich informacji.**

11. O ile większość przepisów dyrektywy o e-prywatności (art. 6, art. 9 itd.) ma zastosowanie tylko do dostawców publicznie dostępnych usług łączności elektronicznej i dostawców publicznych sieci łączności, art. 5 ust. 3 dyrektywy o e-prywatności jest przepisem ogólnym. Ma on zastosowanie nie tylko do usług łączności elektronicznej, lecz także do każdego podmiotu, prywatnego lub publicznego, który wprowadza informacje do urządzenia

[7] Cyberbezpieczeństwo i odporność inteligentnych samochodów; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[8] Rezolucja w sprawie ochrony danych w pojazdach zautomatyzowanych i pojazdach podłączonych do internetu; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.

[9] Dokument roboczy w sprawie pojazdów podłączonych do internetu; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.

[10] Aspekty ochrony danych związane z użytkowaniem pojazdów podłączonych i niepodłączonych do internetu; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.

[11] Zasady cyberbezpieczeństwa dotyczące pojazdów podłączonych do internetu i pojazdów zautomatyzowanych; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[12] Pakiet środków zapewniających zgodność z przepisami na potrzeby odpowiedzialnego wykorzystywania danych w samochodach podłączonych do internetu; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

końcowego lub odczytuje informacje z urządzenia końcowego bez względu na charakter danych przechowywanych lub danych, do których uzyskuje się dostęp.

12. Jeżeli chodzi o pojęcie „urządzenia końcowego", jego definicję zawarto w dyrektywie 2008/63/WE[13]. Zgodnie z art. 1 pkt 1 lit. a) „urządzenie końcowe" oznacza „urządzenie bezpośrednio lub pośrednio podłączone do interfejsu publicznej sieci telekomunikacyjnej w celu przesyłania, przetwarzania lub odbierania informacji; w obydwu przypadkach (połączenia bezpośredniego lub pośredniego), połączenie może być dokonane za pomocą przewodu, światłowodu lub elektromagnetycznie; połączenie jest pośrednie, jeżeli urządzenie jest umieszczone między końcowym urządzeniem telekomunikacyjnym a interfejsem sieci; b) urządzenia naziemnych stacji satelitarnych".

13. W związku z tym, o ile spełnione są powyższe kryteria, pojazd podłączony do internetu i podłączone do niego urządzenie należy uznać za „urządzenie końcowe" (tak samo jak komputer, smartfon czy telewizor z funkcją telewizji hybrydowej), i w stosownych przypadkach zastosowanie mają przepisy art. 5 ust. 3 dyrektywy o e-prywatności.

14. Jak wskazała EROD w swojej opinii 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO[14], art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej stanowi, że co do zasady, i z zastrzeżeniem wyjątków od tej zasady wymienionych w pkt 17 poniżej, aby przechowywać informacje lub uzyskać dostęp do informacji już przechowywanych na urządzeniu końcowym abonenta lub użytkownika, konieczna jest uprzednia zgoda. W zakresie, w jakim informacje przechowywane na urządzeniu użytkownika końcowego są danymi osobowymi, art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma pierwszeństwo przed art. 6 RODO w odniesieniu do czynności przechowywania lub uzyskiwania dostępu do tych informacji[15]. Aby wszelkie późniejsze przetwarzanie danych osobowych następujące po wyżej wymienionych operacjach przetwarzania, w tym przetwarzanie danych osobowych uzyskanych poprzez dostęp do informacji w urządzeniu końcowym, było zgodne z prawem, musi mieć podstawę prawną przewidzianą w art. 6 RODO[16].

15. Ponieważ administrator, ubiegając się o zgodę na przechowywanie informacji albo uzyskanie dostępu do informacji zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności, będzie musiał poinformować osobę, której dane dotyczą, o wszystkich celach przetwarzania – w tym o wszelkich działaniach związanych z przetwarzaniem następujących po wyżej wymienionych operacjach (tj. „późniejszym przetwarzaniem"), zgoda przewidziana w art. 6 RODO będzie najczęściej najbardziej adekwatną podstawą prawną obejmującą przetwarzanie danych osobowych następujące po wspomnianych operacjach (w zakresie, w jakim zgoda osoby, której dane dotyczącą, obejmuje cel późniejszego przetwarzania, zob. pkt 53–54 poniżej). Zgoda będzie zatem prawdopodobnie stanowiła podstawę prawną zarówno dla przechowywania informacji, jak i dla uzyskiwania dostępu do informacji już przechowywanych oraz późniejszego przetwarzania danych osobowych[17]. W istocie przy ocenie zgodności z art. 6 RODO należy wziąć pod uwagę, że cały proces przetwarzania

[13] Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG); https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32008L0063.

[14] Europejska Rada Ochrony Danych, Opinia 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych, przyjęta w dniu 12 marca 2019 r. („opinia 5/2019"), pkt 40;

[15] Ibidem, pkt 40.

[16] Ibidem, pkt 41.

[17] Zgodę wymaganą zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności oraz zgodę potrzebną jako podstawę prawną dla przetwarzania danych (art. 6 RODO) w tym samym konkretnym celu można uzyskać jednocześnie (np. poprzez zaznaczenie pola wyraźnie wskazującego, na co osoba, której dane dotyczą, wyraża zgodę).

obejmuje szczególne czynności, w odniesieniu do których prawodawca UE starał się zapewnić dodatkową ochronę[18]. Ponadto administratorzy danych muszą uwzględniać wpływ na prawa osób, których dane dotyczą, przy określaniu właściwej podstawy prawnej w celu poszanowania zasady rzetelności[19]. Wniosek jest taki, że administratorzy nie mogą polegać na art. 6 RODO w celu ograniczenia dodatkowej ochrony przyznanej na mocy art. 5 ust. 3 dyrektywy o e-prywatności.

16. EROD przypomina, że pojęcie zgody w dyrektywie o e-prywatności pozostaje pojęciem zgody w RODO i musi spełniać wszystkie wymogi dotyczące zgody określone w art. 4 pkt 11 oraz w art. 7 RODO.

17. Jednakże, o ile zgoda jest zasadą, w art. 5 ust. 3 dyrektywy o e-prywatności zezwala się, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym było zwolnione z wymogu świadomej zgody, jeżeli spełnia jedno z następujących kryteriów:

   - **zwolnienie 1:** jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej;
   - **zwolnienie 2:** gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika.

18. W takich przypadkach przetwarzanie danych osobowych, w tym danych osobowych uzyskanych poprzez dostęp do informacji w urządzeniu końcowym, opiera się na jednej z podstaw prawnych określonych w art. 6 RODO. Zgoda nie jest na przykład konieczna w przypadku, gdy przetwarzanie danych jest niezbędne w celu zapewnienia usług nawigacji GPS zażądanych przez osobę, której dane dotyczą, gdyż usługi takie można zaliczyć do usług społeczeństwa informacyjnego.

1.3 Zakres

19. EROD pragnie podkreślić, że niniejsze wytyczne mają na celu ułatwienie przestrzegania przepisów dotyczących przetwarzania danych osobowych przez szerokie grono zainteresowanych stron pracujących w tym otoczeniu. Ich celem nie jest jednak uwzględnienie wszystkich przypadków użytkowania możliwych w tym kontekście ani zapewnienie wskazówek w odniesieniu do każdej możliwej konkretnej sytuacji.

20. Zakres niniejszego dokumentu obejmuje w szczególności przetwarzanie danych osobowych w związku z użytkowaniem do celów pozazawodowych pojazdów podłączonych do internetu przez osoby, których dane dotyczą: np. kierowców, pasażerów, właścicieli pojazdów, innych użytkowników drogi itp. Dokument uwzględnia w szczególności dane osobowe: (i) przetwarzane wewnątrz pojazdu; (ii) wymieniane między pojazdem a podłączonymi do niego urządzeniami przenośnymi (np. smartfonem użytkownika); lub (iii) dane gromadzone lokalnie w pojeździe i eksportowane do podmiotów zewnętrznych (np. producentów pojazdów, zarządców infrastruktury, zakładów ubezpieczeń, warsztatów) na potrzeby dalszego przetwarzania.

21. Definicja pojazdu podłączonego do internetu w rozumieniu tego dokumentu ma szeroki zakres. Pojęcie to można zdefiniować jako pojazd wyposażony w wiele elektronicznych modułów sterujących połączonych za pośrednictwem wewnętrznej sieci pojazdu oraz urządzenia łączności umożliwiające wymianę informacji z innymi urządzeniami zarówno wewnątrz, jak i na zewnątrz pojazdu. Dzięki temu możliwa jest wymiana danych pomiędzy

[18] Opinia 5/2019, pkt 41.

[19] Europejska Rada Ochrony Danych, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, wersja 2.0, 8 października 2019 r., pkt 1.

pojazdem a podłączonymi do niego urządzeniami osobistymi, na przykład poprzez umożliwienie odwzorowania aplikacji mobilnych w urządzeniu informacyjno-rozrywkowym wbudowanym w deskę rozdzielczą samochodu. Ponadto zakres niniejszego dokumentu obejmuje opracowywanie samodzielnych aplikacji mobilnych, tj. niezależnych od pojazdu (np. polegających na wyłącznym korzystaniu ze smartfona), wspomagających kierowców, ponieważ przyczyniają się one do zwiększenia możliwości połączeniowych pojazdu, nawet jeśli nie same w sobie polegają na wymianie danych z pojazdem. Pojazdy podłączone do internetu mają liczne i różnorakie zastosowania, które mogą obejmować[20]:

22. *zarządzanie mobilnością:* funkcje umożliwiające kierowcom szybkie dotarcie do celu w sposób ekonomiczny poprzez zapewnianie aktualnych informacji GPS oraz informacji o potencjalnie niebezpiecznych warunkach pogodowych (np. oblodzonych drogach), natężeniu ruchu lub pracach drogowych, miejscach postoju lub warsztatach, optymalnym zużyciu paliwa lub opłatach za korzystanie z dróg;

23. *zarządzanie pojazdem:* funkcje, które mają pomóc kierowcy w obniżeniu kosztów eksploatacji i zwiększeniu łatwości obsługi, takie jak powiadomienia o stanie pojazdu i przypomnienia o usługach serwisowych, przekazywanie danych dotyczących użytkowania (np. na potrzeby usług naprawy pojazdów), dostosowane do indywidualnych potrzeb ubezpieczenie oparte na mechanizmie „ile jeździsz, tyle płacisz”/uzależnione od stylu jazdy, zdalne sterowanie (np. systemem ogrzewania) lub ustawienia profilowe (np. pozycja siedzenia);

24. *bezpieczeństwo ruchu drogowego:* funkcje ostrzegające kierowcę o zagrożeniach zewnętrznych i informujące o reakcjach wewnętrznych, takie jak ochrona przed zderzeniem, ostrzeżenia o niebezpieczeństwie, ostrzeżenia przed niezamierzoną zmianą pasa ruchu, wykrywanie senności kierowcy, połączenia alarmowe (eCall) lub badanie „czarnych skrzynek” (rejestrator danych na temat zdarzeń) po wypadku;

25. *rozrywka:* funkcje zapewniające kierowcy i pasażerom informacje i rozrywkę, takie jak interfejsy smartfona (połączenia telefoniczne przy użyciu zestawu głośnomówiącego, wiadomości tekstowe generowane głosowo), hotspoty WLAN, muzyka, wideo, internet, media społecznościowe, mobilne biuro lub usługi typu „inteligentny dom”;

26. *wspomaganie kierowcy:* funkcje obejmujące częściowo lub w pełni zautomatyzowane prowadzenie pojazdu, takie jak wsparcie operacyjne lub funkcja autopilota w warunkach dużego natężenia ruchu, podczas parkowania lub na autostradach;

27. *dobre samopoczucie:* funkcje monitorowania komfortu kierowcy, jego zdolności i sprawności do prowadzenia pojazdu, np. wykrywanie zmęczenia lub pomoc medyczna.

28. W związku z powyższym pojazdy mogą być oryginalnie podłączone do internetu lub nie, a dane osobowe mogą być gromadzone na kilka sposobów, m.in. za pośrednictwem: (i) czujników pojazdu; (ii) czarnych skrzynek; lub (iii) aplikacji mobilnych (np. takich, do których dostęp można uzyskać za pośrednictwem urządzenia należącego do kierowcy). Aby aplikacje mobilne wchodziły w zakres niniejszego dokumentu, muszą być związane ze środowiskiem kierowania pojazdem. Na przykład aplikacje do nawigacji GPS spełniają to kryterium. Aplikacje, których funkcjonalność polega jedynie na sugerowaniu kierowcom interesujących miejsc (restauracji, zabytków itp.), nie są objęte zakresem niniejszych wytycznych.

29. Znaczna część danych generowanych przez pojazd podłączony do internetu dotyczy zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w związku z czym stanowią dane osobowe. Na przykład dane obejmują dane umożliwiające bezpośrednią

[20] Strategia PwC „In the fast lane. The bright future of connected cars” [Na pasie szybkiego ruchu. Świetlana przyszłość samochodów podłączonych do internetu], 2014 r.;
https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

identyfikację (np. pełna tożsamość kierowcy), jak również dane umożliwiające identyfikację pośrednią, takie jak szczegółowe informacje dotyczące odbytych podróży, dane dotyczące użytkowania pojazdu (np. dane dotyczące stylu jazdy lub przebytej odległości) lub dane techniczne pojazdu (np. dotyczące zużycia części), które – poprzez porównanie z innymi plikami, a w szczególności z numerem identyfikacyjnym pojazdu (VIN) – można powiązać z daną osobą fizyczną. Dane osobowe gromadzone w pojazdach podłączonych do internetu mogą również obejmować metadane, takie jak informacje o statusie konserwacji pojazdu. Innymi słowy, wszelkie dane, które można powiązać z daną osobą fizyczną, są objęte zakresem niniejszego dokumentu.

30. Ekosystem pojazdów podłączonych do internetu obejmuje szerokie grono zainteresowanych stron. Obejmuje on w szczególności zarówno tradycyjne podmioty sektora motoryzacyjnego, jak i nowe podmioty z branży cyfrowej. Wytyczne te są zatem przeznaczone dla producentów pojazdów i sprzętu oraz dostawców części samochodowych, warsztatów samochodowych, salonów sprzedaży samochodów, dostawców usług w zakresie pojazdów, zarządców flot, zakładów ubezpieczeń motoryzacyjnych, dostawców usług rozrywkowych, operatorów telekomunikacyjnych, zarządców infrastruktury drogowej i organów publicznych, a także osób, których dane dotyczą. EROD podkreśla, że kategorie osób, których dane dotyczą (np. kierowcy, właściciele, pasażerowie itp.), będą się różniły w zależności od rodzaju usługi. Jest to niewyczerpujący wykaz, ponieważ wspomniany ekosystem obejmuje szeroki wachlarz usług, w tym usługi wymagające bezpośredniego uwierzytelnienia lub identyfikacji oraz usługi, w przypadku których nie jest to konieczne.

31. Niektóre czynności związane z przetwarzaniem danych przez osoby fizyczne w pojeździe obywają się „w ramach czynności o czysto osobistym lub domowym charakterze", a zatem nie są objęte zakresem stosowania RODO[21]. Dotyczy to w szczególności wykorzystywania danych osobowych w pojazdach wyłącznie przez osoby, których dane dotyczą i które wprowadziły te dane do urządzenia na desce rozdzielczej pojazdu. EROD przypomina, że zgodnie z motywem 18 RODO rozporządzenie to „ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej".

1.3.1 Poza zakresem niniejszego dokumentu

32. Pracodawcy udostępniający samochody służbowe swoim pracownikom mogą chcieć monitorować działania swoich pracowników (np. w celu zapewnienia bezpieczeństwa pracowników, towarów lub pojazdów, przydzielania zasobów, śledzenia i rozliczania usług lub kontroli czasu pracy). W tym kontekście przetwarzanie danych przez pracodawcę wiąże się ze szczególnymi aspektami w kontekście zatrudnienia, mogącymi podlegać przepisom prawa pracy na szczeblu krajowym, które to przepisy nie mogą zostać wyszczególnione w niniejszych wytycznych[22].

33. Chociaż przetwarzanie danych w kontekście pojazdów komercyjnych wykorzystywanych do celów zawodowych (np. transport publiczny) oraz transportu wspólnego i rozwiązań MaaS może wiązać się ze szczególnymi aspektami, które nie wchodzą w zakres tych ogólnych wytycznych, wiele zasad i zaleceń określonych w tym dokumencie będzie miało zastosowanie również do tych rodzajów przetwarzania.

34. Pojazdy podłączone do internetu są systemami radiowymi i podlegają biernemu śledzeniu, np. przez technologię Wi-Fi lub Bluetooth. Pod tym względem nie różnią się od innych urządzeń podłączonych do internetu i wchodzą w zakres stosowania dyrektywy o e-

[21] Zob. art. 2 ust. 2 lit. c) RODO.

[22] Grupa Robocza Art. 29 szczegółowo opisała tę kwestię w swojej Opinii 2/2017 na temat przetwarzania danych w miejscu pracy (WP 249); https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

prywatności, która podlega obecnie przeglądowi. Wyklucza to zatem również śledzenie na dużą skalę pojazdów wyposażonych w technologię Wi-Fi[23] poprzez gęstą sieć osób postronnych, które korzystają ze wspólnych usług lokalizacji na smartfonach. W ramach tych usług informacje na temat wszystkich widocznych sieci Wi-Fi są rutynowo przekazywane do serwerów centralnych. Ponieważ wbudowany system Wi-Fi może zostać uznany za wtórny identyfikator pojazdu[24], wiąże się to z ryzykiem systematycznego, bieżącego gromadzenia danych na temat kompletnych profili ruchu pojazdów.

35. Pojazdy są coraz częściej wyposażane w urządzenia rejestrujące obraz (np. systemy kamer parkowania lub rejestratory jazdy). Ponieważ wiąże się to z kwestią nagrywania obrazu w miejscach publicznych, co wymaga oceny odpowiednich ram legislacyjnych specyficznych dla każdego państwa członkowskiego, takie przetwarzanie danych nie wchodzi w zakres niniejszych wytycznych.

36. Kwestię przetwarzania danych umożliwiających działanie współpracującego inteligentnego systemu transportowego (C-ITS) – którego definicję określono w dyrektywie 2010/40/UE[25] – omówiono w specjalnej opinii Grupy Roboczej Art. 29[26]. Chociaż definicja C-ITS przedstawiona w dyrektywie nie zawiera żadnych specyfikacji technicznych, w swojej opinii Grupa Robocza Art. 29 skupiła się na komunikatach o niewielkim zasięgu, tj. takich, które nie wymagają interwencji operatora sieci. W szczególności w opinii przedstawiono analizę dotyczącą konkretnych wstępnych możliwości zastosowań i zobowiązano się do dokonania na późniejszym etapie oceny nowych problemów, które niewątpliwie pojawią się, gdy wdrożony zostanie wyższy poziom automatyzacji. Ponieważ skutki dla ochrony danych w kontekście C-ITS są bardzo szczególne (bezprecedensowe ilości danych dotyczących lokalizacji, ciągła transmisja danych osobowych, wymiana danych między pojazdami i innymi obiektami infrastruktury drogowej itp.), a kwestia ta jest nadal omawiana na szczeblu europejskim, przetwarzanie danych osobowych w tym kontekście nie jest objęte zakresem niniejszych wytycznych.

37. Ponadto dokument ten nie ma na celu uwzględnienia wszelkich możliwych kwestii ani odpowiedzi na pytania, które pojawią się w kontekście pojazdów podłączonych do internetu, zatem nie można uznać go za wyczerpujący.

1.4 Definicje

38. **Przetwarzanie** danych osobowych obejmuje wszelkie działania dotyczące danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie itp.[27]

---

[23] Więcej informacji szczegółowych można znaleźć pod adresem: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html

[24] Markus Ullmann, Tobias Franz i Gerd Nolden, „Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings" [Identyfikacja pojazdu na podstawie wtórnego identyfikatora pojazdu – analiza i pomiary w praktyce], VEHICULAR 2017, szósta międzynarodowa konferencja dotycząca postępów w zakresie systemów, technologii i aplikacji samochodowych, Nicea, Francja, 23–27 lipca 2017 r., s. 32–37.

[25] Dyrektywa 2010/40/UE z dnia 7 lipca 2020 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu; https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32010L0040.

[26] Grupa Robocza Art. 29 – Opinia nr 03/2017 dotycząca przetwarzania danych osobowych w ramach współpracujących inteligentnych systemów transportowych (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

[27] Zob. art. 4 pkt 2 RODO.

39. **Osoba, której dane dotyczą**, to osoba fizyczna, której dotyczą przetwarzane dane. W kontekście pojazdów podłączonych do internetu może to być w szczególności kierowca (główny lub okazjonalny), pasażer lub właściciel pojazdu[28].

40. **Administrator danych** to osoba określająca cele i sposoby przetwarzania w pojazdach podłączonych do internetu[29]. Administratorami danych mogą być m.in. dostawcy usług przetwarzający dane z pojazdów na potrzeby przekazywania kierowcom informacji o ruchu, komunikatów na temat ekologicznego stylu jazdy lub ostrzeżeń dotyczących działania pojazdu, informacji o zakładach ubezpieczeń oferujących umowy ubezpieczeniowe oparte na mechanizmie „ile jeździsz, tyle płacisz" lub producenci pojazdów gromadzący dane dotyczące zużycia części pojazdu w celu poprawy jego jakości. Zgodnie z art. 26 RODO co najmniej dwóch administratorów może wspólnie ustalać cele i sposoby przetwarzania – wówczas są oni współadministratorami. W takim przypadku muszą wyraźnie określić swoje odpowiednie obowiązki, szczególnie w zakresie wykonywania praw osób, których dane dotyczą, i przekazywania informacji, o których mowa w art. 13 i 14 RODO.

41. **Podmiot przetwarzający dane** to dowolna osoba przetwarzająca dane osobowe na rzecz i w imieniu administratora danych[30]. Podmiot przetwarzający dane gromadzi i przetwarza dane na polecenie administratora danych, ale nie wykorzystuje ich do celów własnych. Przykładowo w wielu przypadkach producenci sprzętu i dostawcy części samochodowych mogą przetwarzać dane w imieniu producentów pojazdów (co nie oznacza, że nie mogą być administratorami danych do innych celów). Oprócz wymogu, aby podmioty przetwarzające dane wdrożyły odpowiednie środki techniczne i organizacyjne w celu zagwarantowania poziomu bezpieczeństwa dostosowanego do ryzyka, w art. 28 RODO określono obowiązki podmiotu przetwarzającego dane.

42. **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią[31]. Na przykład odbiorcą danych osobowych jest partner handlowy dostawcy usług, który otrzymuje od dostawcy usług dane osobowe wygenerowane z pojazdu. Niezależnie od tego, czy podmioty te działają w roli nowego administratora danych lub podmiotu przetwarzającego dane, muszą spełniać wszystkie obowiązki nałożone przez RODO.

43. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców[32]; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Na przykład organy ścigania mają status upoważnionej strony trzeciej, jeśli zwrócą się o przekazanie danych osobowych w ramach dochodzenia zgodnie z prawem Unii Europejskiej lub państwa członkowskiego.

[28] Zob. art. 4 pkt 1 RODO.
[29] Zob. art. 4 pkt 7 RODO oraz publikacja Europejskiej Rady Ochrony Danych, Wytyczne 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO („wytyczne 07/2020").
[30] Zob. art. 4 pkt 8 RODO oraz wytyczne 07/2020.
[31] Zob. art. 4 pkt 9 RODO oraz wytyczne 07/2020.
[32] Zob. art. 4 pkt 9 i motyw 31 RODO.

1.5 Ryzyko związane z ochroną prywatności i danych

44. Grupa Robocza Art. 29 wyraziła już szereg obaw związanych z systemami internetu rzeczy (IoT), które to obawy mogą również dotyczyć pojazdów podłączonych do internetu[33]. Kwestie związane z bezpieczeństwem i administracją danych, na które zwrócono już uwagę w odniesieniu do IoT, są jeszcze bardziej delikatne w kontekście pojazdów podłączonych do internetu, ponieważ wiążą się z obawami dotyczącymi bezpieczeństwa ruchu drogowego – i mogą mieć wpływ na integralność cielesną kierowcy – w środowisku, które tradycyjnie postrzegane jest jako wyizolowane i chronione przed ingerencjami z zewnątrz.

45. Z pojazdami podłączonymi do internetu wiążą się również poważne obawy dotyczące ochrony danych i prywatności w zakresie przetwarzania danych dotyczących lokalizacji, ponieważ ich coraz bardziej inwazyjny charakter może nadwerężyć obecne możliwości zachowania anonimowości. Europejska Rada Ochrony Danych pragnie położyć szczególny nacisk na fakt, że wykorzystanie technologii lokalizacji wymaga wdrożenia konkretnych zabezpieczeń w celu zapobieżenia nadzorowi osób fizycznych i niewłaściwemu wykorzystaniu danych, a także zwiększyć świadomość zainteresowanych stron w tym zakresie.

1.5.1 Brak kontroli i asymetria informacji

46. Kierowcy i pasażerowie pojazdów mogą nie być zawsze odpowiednio poinformowani o tym, że w pojeździe podłączonym do internetu lub za jego pośrednictwem przetwarzane są dane. Informacje te mogą być przekazywane wyłącznie do właściciela pojazdu, który może nie być kierowcą, a ponadto mogą nie być przekazywane w odpowiednim czasie. Istnieje zatem ryzyko, że oferowane funkcjonalności lub opcje są niewystarczające do sprawowania kontroli niezbędnej do tego, by zainteresowane osoby fizyczne mogły skorzystać z przysługujących im praw w zakresie ochrony danych i prywatności. Aspekt ten ma znaczenie, ponieważ w okresie eksploatacji pojazdy mogą należeć do więcej niż jednego właściciela, ponieważ są sprzedawane albo leasingowane, a nie kupowane.

47. Ponadto, komunikacja w pojeździe może być uruchamiana automatycznie, jak również domyślnie, bez wiedzy użytkownika. W przypadku braku możliwości skutecznego sterowania interakcjami pojazdu i podłączonych do niego urządzeń użytkownikowi będzie niezwykle trudno kontrolować przepływ danych. Jeszcze trudniej będzie mu kontrolować ich późniejsze wykorzystanie, a tym samym zapobiegać możliwej zmianie celu (ang. *function creep*).

1.5.2 Jakość zgody użytkownika

48. EROD podkreśla, że w przypadku gdy przetwarzanie danych odbywa się w oparciu o zgodę, zachowane muszą być wszystkie elementy ważnej zgody, co oznacza, że musi ona być dobrowolna, jednoznaczna i świadoma oraz musi stanowić jednoznaczne okazanie woli osoby, której dane dotyczą, w rozumieniu wytycznych EROD dotyczących zgody[34]. Administratorzy danych muszą zwracać szczególną uwagę na procedury uzyskiwania ważnej zgody od poszczególnych uczestników, m.in. właścicieli lub użytkowników samochodów. Zgoda taka musi zostać udzielona odrębnie i w konkretnym celu oraz nie może być połączona z umową nabycia lub leasingu nowego samochodu. Wycofanie zgody musi być równie łatwe jak jej udzielenie.

49. Te same zasady mają zastosowanie, gdy zgoda jest wymagana w celu spełnienia wymogów dyrektywy o e-prywatności, czyli np. w przypadku przechowywania informacji lub uzyskania dostępu do informacji już przechowywanych w pojeździe, co w niektórych przypadkach jest

[33] Grupa Robocza Art. 29 – Opinia 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu przedmiotów; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pl.pdf

[34] Europejska Rada Ochrony Danych, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, wersja 1.1 z dnia 4 maja 2020 r. („wytyczne 05/2020").

wymagane na mocy art. 5 ust. 3 dyrektywy o e-prywatności. W rzeczywistości, jak wskazano powyżej, zgodę w tym kontekście należy interpretować w świetle przepisów RODO.

50. W wielu sytuacjach użytkownik może nie być świadomy, że w jego pojeździe przetwarzane są dane. Brak takiej informacji stanowi poważną przeszkodę w wykazaniu ważnej zgody w rozumieniu RODO, ponieważ zgoda musi być świadoma. W takich okolicznościach zgody nie można traktować jako podstawy prawnej odpowiedniego przetwarzania danych zgodnie z przepisami RODO.

51. Klasyczne mechanizmy wykorzystywane w celu uzyskania zgody osób mogą być trudne do zastosowania w kontekście pojazdów podłączonych do internetu, co skutkuje zgodą „niskiej jakości" opartą na braku informacji lub faktycznym brakiem możliwości udzielenia precyzyjnie dostosowanej zgody zgodnie z preferencjami wyrażonymi przez osoby fizyczne. W praktyce trudne może być również uzyskanie zgody od kierowców i pasażerów niespokrewnionych z właścicielem pojazdu w przypadku pojazdów z drugiej ręki, leasingowanych, wynajętych lub pożyczonych.

52. W przypadkach, w których dyrektywa o e-prywatności nie wymaga zgody osoby, której dane dotyczą, administrator ma jednak obowiązek dokonania wyboru podstawy prawnej – na podstawie art. 6 RODO – która jest najbardziej odpowiednia w danej sytuacji przetwarzania danych osobowych.

1.5.3 Dalsze przetwarzanie danych osobowych

53. Jeżeli dane są gromadzone na podstawie zgody, której uzyskanie jest wymagane na podstawie art. 5 ust. 3 dyrektywy o e-prywatności, lub na podstawie jednego z wyłączeń określonych w art. 5 ust. 3, a następnie przetwarzane zgodnie z art. 6 RODO, dane te mogą być dalej przetwarzane tylko wtedy, gdy administrator danych zwróci się o dodatkową zgodę na ten inny cel albo gdy administrator danych może wykazać, że przetwarzanie odbywa się na podstawie przepisów prawa Unii lub państwa członkowskiego w celu zagwarantowania celów, o których mowa w art. 23 ust. 1 RODO[35]. EROD uważa, że dalsze przetwarzanie na podstawie testu zgodności zgodnie z art. 6 ust. 4 RODO nie jest możliwe w takich przypadkach, ponieważ podważałoby normę dotyczącą ochrony danych określoną w dyrektywie o e-prywatności. W rzeczywistości w przypadkach, w których na podstawie dyrektywy o e-prywatności zgoda jest wymagana, musi ona być jednoznaczna i świadoma, czyli osoby, których dane dotyczą, muszą być świadome każdego celu przetwarzania danych i mieć prawo do odmowy zgody na określony cel[36]. Stwierdzenie, że dalsze przetwarzanie na podstawie testu zgodności zgodnie z art. 6 ust. 4 RODO jest możliwe, stanowiłoby obejście samej zasady wymogów dotyczących zgody ustanowionych w obowiązującej dyrektywie.

54. EROD przypomina, że początkowa zgoda nigdy nie będzie uzasadniała dalszego przetwarzania, ponieważ zgoda musi być świadoma i jednoznaczna, aby była ważna.

55. Na przykład dane telemetryczne, które są gromadzone podczas użytkowania pojazdu do celów konserwacji, nie mogą być ujawniane bez zgody użytkowników zakładom ubezpieczeń pojazdów na potrzeby tworzenia profili kierowców, aby oferować polisy ubezpieczeniowe oparte na zachowaniu kierowcy.

56. Ponadto dane gromadzone w pojazdach podłączonych do internetu mogą być przetwarzane przez organy ścigania w celu wykrywania przypadków przekraczania dopuszczalnej prędkości lub innych naruszeń prawa, pod warunkiem że spełnione są szczególne warunki określone w dyrektywie o ochronie danych w sprawach karnych. W takim przypadku dane uznaje się za dotyczące wyroków skazujących i przestępstw podlegających warunkom

[35] Zob. również Europejska Rada Ochrony Danych, Wytyczne 10/2020 w sprawie ograniczeń praw osób, których dane dotyczą, na podstawie art. 23 RODO.
[36] Zob. sekcje 3.2 i 3.3 wytycznych 05/2020.

określonym w art. 10 RODO i innych właściwych przepisach krajowych. Producenci mogą przekazywać takie dane organom ścigania, jeżeli spełnione są konkretne warunki takiego przetwarzania. EROD zwraca uwagę, że przetwarzanie danych osobowych wyłącznie w celu spełniania żądań organów ścigania nie kwalifikuje się jako konkretny, wyraźny i prawnie uzasadniony cel w rozumieniu art. 5 ust. 1 lit. b) RODO. Jeżeli organy ścigania są w świetle prawa do tego uprawnione, mogą występować w roli stron trzecich w rozumieniu art. 4 pkt 10 RODO – w takich przypadkach producenci byliby uprawnieni do przekazania im wszelkich danych, którymi dysponują, z zastrzeżeniem zachowania zgodności z odpowiednimi ramami prawnymi w każdym państwie członkowskim.

1.5.4 Nadmierne gromadzenie danych

57. W miarę jak w pojazdach podłączonych do internetu instaluje się coraz więcej czujników, wzrasta ryzyko nadmiernego gromadzenia danych w stosunku do tego, co jest niezbędne do osiągnięcia danego celu.

58. Opracowanie nowych funkcjonalności, w szczególności opartych na algorytmach uczenia się maszyn, może wymagać dużych ilości danych gromadzonych przez długi czas.

1.5.5 Bezpieczeństwo danych osobowych

59. Mnogość funkcjonalności, usług i interfejsów (np. web, USB, RFID, Wi-Fi) oferowanych przez pojazdy podłączone do internetu prowadzi do zmniejszenia odporności na ataki, a tym samym zwiększenia liczby potencjalnych słabych punktów, przez które może dojść do naruszenia danych osobowych. W przeciwieństwie do większości urządzeń IoT pojazdy podłączone do internetu są krytycznymi systemami, w przypadku których naruszenie bezpieczeństwa może zagrażać życiu ich użytkowników i innych osób z ich otoczenia. Tym większe w tym kontekście znaczenie ma ograniczenie ryzyka wykorzystania słabych punktów pojazdów podłączonych do internetu przez hakerów.

60. Dodatkowo dane osobowe przechowywane w pojazdach lub poza nimi (np. w infrastrukturach umożliwiających przetwarzanie w chmurze) należy odpowiednio zabezpieczyć przed nieuprawnionym dostępem. Na przykład na czas konserwacji pojazd musi zostać przekazany technikowi, który będzie potrzebował dostępu do niektórych danych technicznych samochodu. O ile technik rzeczywiście potrzebuje dostępu do takich danych technicznych, istnieje ryzyko, że mógłby on spróbować uzyskać dostęp do wszystkich danych przechowywanych w pojeździe.

2 ZALECENIA OGÓLNE

61. Aby ograniczyć ryzyko dla wymienionych wyżej osób, których dane dotyczą, producenci pojazdów i sprzętu, dostawcy usług lub wszelkie inne zainteresowane strony, które mogą pełnić funkcję administratora danych lub podmiotu przetwarzającego dane w odniesieniu do pojazdów podłączonych do internetu, powinni przestrzegać poniższych zaleceń ogólnych.

2.1 Kategorie danych

62. Jak wspomniano we wstępie, większość danych związanych z pojazdami podłączonymi do internetu uznaje się za dane osobowe w zakresie, w jakim możliwe jest powiązanie ich z co najmniej jedną możliwą do zidentyfikowania osobą. Obejmuje to dane techniczne dotyczące ruchu pojazdu (np. prędkość, przebyta droga) oraz stanu pojazdu (np. temperatura płynu chłodzącego silnik, liczba obrotów na minutę, ciśnienie w oponach). Niektóre dane wygenerowane przez pojazdy podłączone do internetu mogą również wymagać szczególnej uwagi ze względu na ich wrażliwy charakter lub potencjalny wpływ na prawa i interesy osób, których dane dotyczą. Obecnie EROD wyodrębniła trzy kategorie danych osobowych wymagających szczególnej uwagi ze strony producentów pojazdów i sprzętu, dostawców usług i innych administratorów danych: dane dotyczące lokalizacji, dane biometryczne (oraz

wszelkie szczególne kategorie danych osobowych określone w art. 9 RODO) oraz dane, które mogłyby ujawniać popełnienie przestępstwa lub naruszenie przepisów ruchu drogowego.

2.1.1 Dane dotyczące lokalizacji

63. Gromadząc dane osobowe, producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni pamiętać o tym, że dane dotyczące lokalizacji w szczególny sposób ujawniają informacje na temat codziennych nawyków osób, których dane te dotyczą. Dane na temat odbytych przejazdów są bardzo charakterystyczne, ponieważ dzięki nim można wyciągnąć wnioski dotyczące miejsca pracy i zamieszkania kierowcy, a także jego zainteresowań (czasu wolnego), i mogą one potencjalnie ujawniać informacje wrażliwe, np. na temat wyznania – na podstawie miejsca kultu – lub orientacji seksualnej – na podstawie odwiedzanych miejsc. W związku z tym producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni zachować szczególną ostrożność, aby nie gromadzić danych dotyczących lokalizacji, chyba że jest to absolutnie niezbędne do celów przetwarzania. Na przykład gdy przetwarzanie polega na wykrywaniu ruchu pojazdu, żyroskop jest wystarczającym narzędziem do spełnienia tej funkcji, bez potrzeby zbierania danych dotyczących lokalizacji.

64. Ogólnie rzecz biorąc, gromadzenie danych dotyczących lokalizacji również wiąże się z koniecznością przestrzegania następujących zasad:

- odpowiednia konfiguracja częstotliwości dostępu do danych dotyczących lokalizacji i poziomu ich szczegółowości w stosunku do celu przetwarzania. Na przykład aplikacja pogodowa nie powinna mieć możliwości dostępu do lokalizacji pojazdu w każdej sekundzie, nawet za zgodą osoby, której dane dotyczą;
- przekazywanie prawidłowych informacji dotyczących celu przetwarzania (np. czy przechowuje się historię lokalizacji, a jeżeli tak, to w jakim celu);
- gdy przetwarzanie odbywa się na podstawie udzielonej zgody – uzyskanie ważnej (dobrowolnej, świadomej i jednoznacznej) zgody, która jest odrębna w stosunku do ogólnych warunków sprzedaży lub użytkowania, na przykład w komputerze pokładowym;
- uruchamianie usług lokalizacji tylko wtedy, gdy użytkownik włączy funkcjonalność, która wymaga informacji o lokalizacji pojazdu, a nie w sposób domyślny i ciągły po uruchomieniu samochodu;
- informowanie użytkownika o tym, że usługi lokalizacji zostały włączone, w szczególności za pomocą ikon (np. strzałki poruszającej się po ekranie);
- dostępność opcji umożliwiającej wyłączenie usług lokalizacji w dowolnym momencie;
- określenie ograniczonego czasu przechowywania danych.

2.1.2 Dane biometryczne

65. W kontekście pojazdów podłączonych do internetu dane biometryczne wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej mogą być przetwarzane, w zakresie zgodnym z art. 9 RODO i z zastrzeżeniem krajowych wyjątków, między innymi w celu umożliwienia dostępu do pojazdu, uwierzytelnienia tożsamości kierowcy/właściciela lub udzielenia dostępu do ustawień i preferencji profilu kierowcy. Jeżeli chodzi o wykorzystywanie danych biometrycznych, zagwarantowanie osobie, której dane dotyczą, pełnej kontroli nad jej danymi wiąże się z jednej strony z koniecznością zapewnienia alternatywnego rozwiązania nieopartego na danych biometrycznych (np. wykorzystania fizycznego klucza lub kodu) bez dodatkowych ograniczeń (tzn. wykorzystanie danych biometrycznych nie powinno być obowiązkowe), a z drugiej strony z przechowywaniem i porównywaniem wzoru biometrycznego w zaszyfrowanej postaci wyłącznie na poziomie

lokalnym, przy czym dane biometryczne nie są przetwarzane przez zewnętrzny terminal odczytujący/ porównujący dane.

66. W przypadku danych biometrycznych[37] istotne jest zapewnienie, aby rozwiązanie umożliwiające uwierzytelnianie za pomocą danych biometrycznych było wystarczająco niezawodne, w szczególności poprzez zastosowanie się do poniższych zasad:

- ustawienia stosowanego rozwiązania opartego na danych biometrycznych (np. współczynnik wyników fałszywie dodatnich i fałszywie ujemnych) są dostosowane do poziomu bezpieczeństwa wymaganej kontroli dostępu;
- stosowane rozwiązanie oparte na danych biometrycznych wykorzystuje czujnik odporny na ataki (np. na wykorzystanie specjalnego wydruku odcisku palca do rozpoznawania odcisków palców);
- liczba prób uwierzytelnienia jest ograniczona;
- wzór/model biometryczny jest przechowywany w pojeździe, w zaszyfrowanej postaci wykorzystującej algorytm kryptograficzny i zarządzanie kluczem na poziomie odpowiadającym aktualnemu stanowi techniki;
- surowe dane wykorzystywane do stworzenia wzoru biometrycznego i uwierzytelnienia użytkownika są przetwarzane w czasie rzeczywistym i nie są przechowywane, nawet lokalnie.

2.1.3 Dane ujawniające przestępstwa lub inne naruszenia

67. Do celów przetwarzania danych związanych z potencjalnymi naruszeniami prawa w rozumieniu art. 10 RODO Europejska Rada Ochrony Danych zaleca, aby dane były przetwarzane lokalnie – w takim przypadku osoba, której dane dotyczą, ma pełną kontrolę nad takim przetwarzaniem (zob. omówienie lokalnego przetwarzania w sekcji 2.4). Poza pewnymi wyjątkami (zob. analiza przykładu na temat badań wypadkowości przedstawiona w sekcji 3.3) zewnętrzne przetwarzanie danych ujawniających przestępstwa lub inne naruszenia jest zabronione. W związku z tym w zależności od wrażliwości danych należy wdrożyć solidne środki bezpieczeństwa, na przykład takie, jakie opisano w sekcji 2.7, aby zapewnić ochronę przed nieuprawnionym dostępem, zmianą i usunięciem takich danych.

68. Niektóre kategorie danych osobowych pochodzące z pojazdów podłączonych do internetu mogłyby ujawnić, że doszło lub dochodzi do popełnienia przestępstwa lub innego naruszenia („dane związane z naruszeniem prawa"), a tym samym podlegać szczególnym ograniczeniom (np. dane wskazujące na to, że pojazd przejechał przez linię ciągłą, dane dotyczące prędkości chwilowej pojazdu połączone z dokładnymi danymi dotyczącymi lokalizacji). W szczególności w razie gdyby takie dane były przetwarzane przez właściwy organ krajowy do celów prowadzenia dochodzeń i ścigania przestępstw, zastosowanie miałyby zabezpieczenia, o których mowa w art. 10 RODO.

2.2 Cele

69. Dane osobowe mogą być przetwarzane w wielu różnych celach w związku z pojazdami podłączonymi do internetu, w tym na potrzeby zapewnienia bezpieczeństwa kierowcy, ubezpieczenia, skutecznego transportu, rozrywki lub usług informacyjnych. Zgodnie z wymogami przewidzianymi w art. 5 RODO administratorzy danych muszą zapewnić, aby ich cele przetwarzania były „konkretne, wyraźne i prawnie uzasadnione", aby dane nie podlegały dalszemu przetwarzaniu w sposób niezgodny z tymi celami oraz aby istniała ważna podstawa prawna przetwarzania. W części III niniejszych wytycznych omówiono kilka konkretnych przykładów celów, które mogą realizować administratorzy danych działający

[37] Zakaz przewidziany w art. 9 ust. 1 RODO dotyczy wyłącznie przetwarzania „danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej".

w kontekście pojazdów podłączonych do internetu, a także przedstawiono konkretne zalecenia w odniesieniu do każdego rodzaju przetwarzania.

2.3 Znaczenie i minimalizacja danych

70. W celu zapewnienia zgodności z zasadą minimalizacji danych[38] producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni zwracać szczególną uwagę na kategorie danych, których potrzebują z pojazdu podłączonego do internetu, ponieważ mogą oni gromadzić wyłącznie te dane osobowe, które są istotne i niezbędne do celów przetwarzania. Na przykład dane dotyczące lokalizacji są szczególnie inwazyjne i mogą ujawniać informacje na temat wielu codziennych nawyków osób, których dane te dotyczą. W związku z tym uczestnicy rynku powinni zachować szczególną ostrożność, aby nie gromadzić danych dotyczących lokalizacji, chyba że jest to absolutnie niezbędne do celów przetwarzania (zob. omówienie danych dotyczących lokalizacji w sekcji 2.1 powyżej).

2.4 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

71. Zważywszy na ilość i różnorodność danych osobowych generowanych przez pojazdy podłączone do internetu, EROD zauważa, że administratorzy danych są zobowiązani do zapewnienia, aby technologie wdrażane w kontekście pojazdów podłączonych do internetu były skonfigurowane w sposób zapewniający poszanowanie prywatności osób poprzez zastosowanie obowiązków dotyczących uwzględnienia ochrony danych już w fazie projektowania i domyślnej ochrony danych zgodnie z wymogami określonymi w art. 25 RODO. Technologie należy projektować tak, aby ograniczyć do minimum gromadzenie danych osobowych, zapewnić domyślne ustawienia umożliwiające ochronę prywatności oraz zagwarantować, że osoby, których dane dotyczą, są odpowiednio informowane i mają możliwość łatwego modyfikowania ustawień dotyczących ich danych osobowych. Konkretne wytyczne dotyczące tego, w jaki sposób producenci i dostawcy usług mogą dopełnić obowiązku uwzględnienia ochrony danych już w fazie projektowania i domyślnej ochrony danych, mogłyby być korzystne dla podmiotów z branży oraz zewnętrznych dostawców aplikacji.

72. Niektóre opisane niżej ogólne praktyki również mogą się przyczynić do ograniczenia ryzyka naruszenia praw lub wolności osób fizycznych związanego z pojazdami podłączonymi do internetu[39].

2.4.1 Lokalne przetwarzanie danych osobowych

73. Ogólnie producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni w miarę możliwości stosować procesy, które nie wiążą się z wykorzystywaniem danych osobowych lub ich przekazywaniem poza pojazd (tj. dane są przetwarzane wewnętrznie). Charakter pojazdów podłączonych do internetu pociąga jednak za sobą ryzyko związane np. z możliwymi atakami podmiotów zewnętrznych na lokalne operacje przetwarzania danych lub wyciekiem danych lokalnych w wyniku sprzedaży części pojazdu. W związku z tym należy poświęcić odpowiednią uwagę i wdrożyć odpowiednie środki bezpieczeństwa, aby zagwarantować, że przetwarzanie lokalne zachowa swój lokalny charakter. Scenariusz ten ma tę zaletę, że gwarantuje użytkownikowi wyłączną i pełną kontrolę nad jego danymi osobowymi i jako taki „w fazie projektowania" stwarza mniejsze ryzyko dla prywatności, w szczególności dzięki zakazowi jakiegokolwiek przetwarzania danych przez zainteresowane strony bez wiedzy osoby, której dane dotyczą. Umożliwia on również przetwarzanie danych wrażliwych, takich jak dane biometryczne lub dane dotyczące przestępstw lub innych naruszeń, a także szczegółowych danych dotyczących lokalizacji,

[38] Art. 5 ust. 1 lit. c) RODO.

[39] Zob. również Europejska Rada Ochrony Danych, Wytyczne 4/2019 dotyczące artykułu 25 – Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, przyjęte w dniu 20 października 2020 r. („wytyczne 4/2019").

które w przeciwnym razie podlegałyby bardziej rygorystycznym przepisom (zob. poniżej). Dodatkowo wiąże się on z mniejszym ryzykiem w cyberprzestrzeni i z niewielkimi opóźnieniami, co sprawia, że szczególnie dobrze nadaje się do funkcji zautomatyzowanego wspomagania jazdy. Niektóre przykłady tego typu rozwiązań mogą obejmować:

- aplikacje wspierające ekologiczny styl jazdy, które przetwarzają dane w pojeździe w celu wyświetlania w czasie rzeczywistym na ekranie pokładowym wskazówek dotyczących ekologicznego stylu jazdy;
- aplikacje, które przekazują dane osobowe do urządzenia takiego jak smartfon pod pełną kontrolą użytkownika (na przykład za pośrednictwem technologii Bluetooth lub Wi-Fi), ale które nie przekazują danych dotyczących pojazdu dostawcom aplikacji ani producentom pojazdów; obejmuje to na przykład parowanie smartfonów w celu korzystania z ekranu w samochodzie, systemów multimedialnych, mikrofonu (lub innych czujników) do rozmów telefonicznych itp. w zakresie, w jakim gromadzone dane pozostają pod kontrolą osoby, której dane dotyczą, i są wykorzystywane wyłącznie do świadczenia wybranej przez nią usługi;
- aplikacje zwiększające bezpieczeństwo wbudowane w pojazdach, takie jak te, które przekazują kierowcy sygnały dźwiękowe lub wibracje, gdy wyprzedza on samochód bez kierunkowskazu lub przejeżdża przez linię ciągłą, lub które wysyłają powiadomienia dotyczące stanu pojazdu (np. powiadomienie o zużyciu klocków hamulcowych);
- aplikacje do odblokowywania, uruchamiania lub aktywowania określonych komend dla pojazdu przy użyciu danych biometrycznych kierowcy przechowywanych w pojeździe (takich jak wizerunek twarzy, modele głosowe lub minucje).

74. Aplikacje takie jak te wymienione powyżej przetwarzają dane w celu wykonywania przez daną osobę działań o charakterze czysto osobistym (tj. bez przekazywania danych osobowych administratorowi danych lub podmiotowi przetwarzającemu dane). W związku z tym zgodnie z art. 2 ust. 2 RODO **aplikacje te nie wchodzą w zakres stosowania RODO.**

75. Niemniej, o ile RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, jego przepisy mają zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki do przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej (producentów samochodów, dostawców usług itp.) zgodnie z motywem 18 RODO. W związku z tym, gdy wymienione wyżej podmioty są administratorami danych lub podmiotami przetwarzającymi dane, muszą one opracowywać bezpieczne aplikacje samochodowe z należytym poszanowaniem zasady uwzględnienia ochrony prywatności już w fazie projektowania oraz domyślnej ochrony prywatności. W każdym wypadku zgodnie z motywem 78 RODO „[j]eżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych”[40]. Z jednej strony usprawni to rozwój usług skoncentrowanych na użytkowniku, a z drugiej strony ułatwi i zabezpieczy wszelkie dalsze zastosowania w przyszłości, które mogą ponownie wejść w zakres stosowania RODO. Ściślej mówiąc, EROD zaleca stworzenie bezpiecznej platformy aplikacji samochodowych, fizycznie oddzielonej funkcji samochodu od związanych z bezpieczeństwem, tak aby dostęp do

[40] Więcej zaleceń dotyczących uwzględniania ochrony prywatności już w fazie projektowania i domyślnej ochrony prywatności przedstawiono w wytycznych 4/2019.

danych samochodu nie zależał od zewnętrznych możliwości chmury, które nie są w danym przypadku niezbędne.

76. Producenci samochodów i dostawcy usług powinni w miarę możliwości rozważać lokalne przetwarzanie danych w celu ograniczenia potencjalnego ryzyka związanego z przetwarzaniem w chmurze, na które zwrócono uwagę w opinii w sprawie przetwarzania w chmurze wydanej przez Grupę Roboczą Art. 29[41].

77. Zasadniczo użytkownicy powinni mieć możliwość kontrolowania sposobu gromadzenia i przetwarzania ich danych w pojeździe:

- informacje dotyczące przetwarzania muszą być dostępne w języku kierowcy (instrukcja obsługi, ustawienia itp.);
- EROD zaleca, aby domyślnie przetwarzane były tylko dane ściśle niezbędne do funkcjonowania pojazdu. Osoby, których dane dotyczą, powinny mieć możliwość aktywowania lub dezaktywowania usług przetwarzania danych w odniesieniu do każdego innego celu i administratora/podmiotu przetwarzającego, a także powinny móc usuwać dane objęte przetwarzaniem, z uwzględnieniem celu i podstawy prawnej przetwarzania danych;
- danych nie należy przekazywać osobom trzecim (użytkownik ma wyłączny dostęp do tych danych);
- dane należy przechowywać jedynie tak długo, jak jest to konieczne do świadczenia usługi lub w inny sposób wymagane przez prawo Unii lub państwa członkowskiego;
- osoby, których dane dotyczą, powinny mieć możliwość trwałego usunięcia wszelkich danych osobowych przed wystawieniem pojazdów na sprzedaż;
- osoby, których dane dotyczą, powinny mieć w miarę możliwości bezpośredni dostęp do danych generowanych przez te aplikacje.

78. Ponadto, o ile nie w każdym przypadku użytkowania lokalne przetwarzanie danych jest możliwe, często można zastosować rozwiązanie polegające na „przetwarzaniu hybrydowym". Na przykład w kontekście ubezpieczenia opartego na użytkowaniu (ang. *usage-based insurance*) dane osobowe dotyczące zachowania kierowcy (np. siła, z jaką naciska pedał hamulca, pokonywany dystans itp.) mogłyby być przetwarzane albo wewnątrz pojazdu, albo przez dostawcę usług telematycznych w imieniu zakładu ubezpieczeń (administratora danych) w celu wygenerowania wyników liczbowych, które są przekazywane do zakładu ubezpieczeń w określonych interwałach (np. co miesiąc). W ten sposób zakład ubezpieczeń nie uzyskuje dostępu do surowych danych dotyczących zachowań, a jedynie do zbiorczego zestawu, który jest wynikiem przetwarzania. Zapewnia to zgodność z zasadami minimalizacji danych już w fazie projektowania. Oznacza to również, że użytkownicy muszą mieć możliwość wykonania swoich praw, gdy dane przechowują inne podmioty: na przykład użytkownik powinien móc usunąć dane przechowywane w systemach warsztatu samochodowego lub salonu sprzedaży na warunkach określonych w art. 17 RODO.

2.4.2 Anonimizacja i pseudominizacja

79. W sytuacji, gdy przewiduje się przekazywanie danych osobowych poza pojazd, należy rozważyć ich anonimizację przed przekazaniem. Podczas anonimizacji administrator powinien wziąć pod uwagę wszystkie operacje przetwarzania, które mogłyby potencjalnie prowadzić do ponownej identyfikacji danych, jak np. przekazywanie lokalnie zanonimizowanych danych. EROD przypomina, że zasady ochrony danych nie mają

[41] Grupa Robocza Art. 29 – Opinia 5/2012 w sprawie przetwarzania w chmurze; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_pl.pdf

zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować[42]. Gdy zbiór danych jest już faktycznie zanonimizowany i nie ma już możliwości zidentyfikowania poszczególnych osób fizycznych, prawo UE o ochronie danych nie ma dalej zastosowania. W związku z tym anonimizacja w stosownych przypadkach może być dobrą strategią pozwalającą zachować korzyści i ograniczyć ryzyko związane z pojazdami podłączonymi do internetu.

80. Jak wyszczególniono w opinii Grupy Roboczej Art. 29 w sprawie technik anonimizacji, w celu osiągnięcia anonimizacji danych można stosować różne metody, a czasami połączenie kilku z nich[43].

81. Inne techniki, jak np. pseudonimizacja[44], mogą pomóc ograniczyć ryzyko związane z przetwarzaniem danych, biorąc pod uwagę fakt, że w większości przypadków dane umożliwiające bezpośrednią identyfikację nie są niezbędne do osiągnięcia celu przetwarzania. Pseudonimizacja, jeżeli jest wzmocniona zabezpieczeniami, poprawia ochronę danych osobowych dzięki ograniczeniu ryzyka ich niewłaściwego wykorzystania. W przeciwieństwie do anonimizacji pseudonimizacja jest odwracalna, a dane pseudonimiczne uznaje się za dane osobowe podlegające RODO.

2.4.3 Oceny skutków dla ochrony danych

82. Biorąc pod uwagę skalę i wrażliwość danych osobowych, które mogą być generowane przez pojazdy podłączone do internetu, istnieje prawdopodobieństwo, że przetwarzanie – w szczególności w sytuacjach, w których dane osobowe przetwarza się poza pojazdem – będzie często powodować znaczne ryzyko dla praw i wolności osób fizycznych. W takim przypadku uczestnicy sektora będą zobowiązani do przeprowadzenia oceny skutków dla ochrony danych w celu określenia i ograniczenia ryzyka, jak określono w art. 35 i 36 RODO. Nawet w przypadkach, w których ocena skutków dla ochrony danych nie jest wymagana, najlepszą praktyką jest przeprowadzenie jej na jak najwcześniejszym etapie projektowania. Dzięki temu uczestnicy sektora będą mogli uwzględnić wyniki tej analizy w ich wyborach dotyczących projektowania jeszcze przed wprowadzeniem nowych technologii.

2.5 Informacje

83. Przed przystąpieniem do przetwarzania danych osobowych osoba, której dane dotyczą, musi zostać uzyskać informacje o tożsamości administratora danych (np. producenta pojazdów i sprzętu lub dostawcy usług), celu przetwarzania, odbiorcach danych, okresie przechowywania danych oraz przysługujących jej prawach wynikających z RODO[45].

84. Ponadto producent pojazdu i sprzętu, dostawca usług lub inny administrator danych powinien również przekazać osobie, której dane dotyczą, następujące informacje, sformułowane w sposób jasny, prosty i łatwo dostępny:

- dane kontaktowe inspektora ochrony danych;
- cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;

[42] Zob. art. 4 pkt 1 i motyw 26 RODO.
[43] Grupa Robocza Art. 29, Opinia 05/2014 w sprawie technik anonimizacji; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf
[44] Art. 4 pkt 5 RODO. Sprawozdanie Agencji UE ds. Cyberbezpieczeństwa opublikowane w dniu 3 grudnia 2019 r.; https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
[45] Art. 5 ust. 1 lit. a) i art. 13 RODO. Zob. również Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679 (wp260rev.01), zatwierdzone przez EROD.

- wyraźne określenie prawnie uzasadnionych interesów realizowanych przez administratora lub przez podmiot zewnętrzny, gdy takie prawnie uzasadnione interesy stanowią podstawę prawną przetwarzania;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- informacje o prawie do wycofania zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, gdy przetwarzanie danych odbywa się na podstawie zgody;
- w stosownych przypadkach informacje o tym, że administrator zamierza przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej, a także o zabezpieczeniach zastosowanych w celu przekazania tych danych;
- informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, które wywołuje skutki prawne w odniesieniu do osoby, której dane dotyczą, lub w podobny sposób znacząco na nią wpływa, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Może to mieć miejsce w szczególności w odniesieniu do oferowania osobom fizycznym ubezpieczeń opartych na użytkowaniu;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informacje o dalszym przetwarzaniu;
- w przypadku współadministracji – jasne i pełne informacje o obowiązkach każdego administratora danych.

85. W niektórych przypadkach dane osobowe nie są zbieranie bezpośrednio od danej osoby fizycznej, której dotyczą. Na przykład producent pojazdów i sprzętu może polegać na sprzedawcy w zakresie gromadzenia informacji o właścicielu pojazdu w celu zaoferowania usług awaryjnej pomocy drogowej. Jeżeli dane nie zostały zebrane bezpośrednio, producent pojazdów i sprzętu, dostawca usług lub inny administrator danych, oprócz informacji wymienionych powyżej, wskazuje również kategorie odnośnych danych osobowych, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Administrator danych przekazuje te informacje w rozsądnym terminie po uzyskaniu danych, lecz **nie później niż w pierwszym z następujących terminów** zgodnie z art. 14 ust. 3 RODO: (i) w ciągu miesiąca po pozyskaniu danych, mając na uwadze konkretne okoliczności przetwarzania danych osobowych, (ii) przy pierwszej komunikacji z osobą, której dane dotyczą lub (iii) jeśli dane te są przekazywane stronie trzeciej, przed przekazaniem danych.

86. Konieczne może być również dostarczenie nowych informacji osobom, których dane dotyczą, w przypadku gdy będzie się nimi zajmował nowy administrator danych. Usługę pomocy drogowej, która współdziała z pojazdami podłączonymi do internetu, mogą świadczyć różni administratorzy danych, w zależności od tego, w jakim państwie lub regionie

wymagana jest pomoc. Nowi administratorzy danych powinni przekazywać osobom, których dane dotyczą, wymagane informacje, gdy osoby te przekraczają granice i gdy usługi współdziałające z pojazdami podłączonymi do internetu są świadczone przez nowych administratorów danych.

87. Informacje kierowane do osób, których dane dotyczą, mogą być przekazywane warstwowo[46], tj. poprzez wyodrębnienie dwóch poziomów informacji: z jednej strony informacji pierwszego poziomu, które są najważniejsze dla osób, których dane dotyczą, a z drugiej strony informacji, które przypuszczalnie przydadzą się na późniejszym etapie. Istotne informacje pierwszego poziomu obejmują, oprócz tożsamości administratora danych, cel przetwarzania i opis praw osoby, której dane dotyczą, a także wszelkie dodatkowe informacje na temat przetwarzania, które ma największy wpływ na osobę, której dane dotyczą, oraz przetwarzania, które może ją zaskoczyć. EROD zaleca, aby w kontekście pojazdów podłączonych do internetu osoba, której dane dotyczą, została powiadomiona o wszystkich odbiorcach w ramach pierwszego poziomu informacji. Jak stwierdzono w wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości, administratorzy muszą udzielić informacji o odbiorcach, która jest najbardziej istotna dla osób, których dane dotyczą. W praktyce będą to głównie nazwani odbiorcy, tak by osoby, których dane dotyczą, dokładnie wiedziały, kto posiada ich dane osobowe. Jeżeli administratorzy nie są w stanie podać nazw odbiorców, informacja powinna być tak szczegółowa, jak jest to możliwe, wskazując rodzaj odbiorcy (tj. odnosząc się do wykonywanych przez niego działań), przemysł, sektor i podsektor oraz lokalizację odbiorców.

88. Osoby, których dane dotyczą, mogą być informowane za pomocą zwięzłych i łatwo zrozumiałych klauzul w umowie sprzedaży pojazdu, w umowie o świadczenie usług lub w dowolnej formie pisemnej, przy użyciu odrębnych dokumentów (np. książki serwisowej lub instrukcji obsługi pojazdu) albo komputera pokładowego.

89. Jako uzupełnienie niezbędnych informacji, zgodnie z wymogami art. 13 i 14 RODO, można by stosować standardowe ikony w celu zwiększenia przejrzystości poprzez potencjalne ograniczenie konieczności przedstawiania osobie, której dane dotyczą, znacznych ilości pisemnych informacji. Powinny one być widoczne w pojazdach, aby zapewnić odpowiedni, zrozumiały i czytelny obraz sytuacji w odniesieniu do planowanego przetwarzania. EROD podkreśla znaczenie standaryzacji tych ikon w celu zapewnienia użytkownikowi tych samych symboli niezależnie od marki lub modelu pojazdu. Na przykład, w przypadku gdy gromadzone są określone rodzaje danych, takie jak dane dotyczące lokalizacji, komputery pokładowe pojazdów mogłyby wyraźnie informować (np. za pomocą lampki wewnątrz pojazdu) pasażerów o odbywającym się gromadzeniu danych.

2.6 Prawa osoby, której dane dotyczą

90. Producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni ułatwiać osobom, których dane dotyczą, kontrolę nad ich danymi przez cały okres przetwarzania, wdrażając konkretne narzędzia zapewniające skuteczny sposób wykonywania ich praw, w szczególności prawa dostępu, prawa do sprostowania, usuwania, ograniczenia przetwarzania oraz, w zależności od podstawy prawnej przetwarzania, prawa do przenoszenia danych i prawa do sprzeciwu.

91. Aby ułatwić zmianę ustawień, należy wdrożyć system zarządzania profilami na potrzeby zapisywania preferencji znanych kierowców i zapewnienia im możliwości łatwej zmiany ustawień prywatności w dowolnym momencie. System zarządzania profilami powinien gromadzić w jednym miejscu wszystkie ustawienia dotyczące danych dla każdej operacji przetwarzania danych, w szczególności w celu ułatwienia dostępu do danych osobowych

[46] Zob. Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na mocy rozporządzenia 2016/679 (wp260rev.01), zatwierdzone przez EROD.

z systemów pojazdów, kasowania i usuwania tych danych oraz ich przenoszenia na wniosek osoby, której dane dotyczą. Kierowcy powinni mieć możliwość wstrzymania gromadzenia niektórych rodzajów danych – tymczasowo lub na stałe – w dowolnym momencie, chyba że istnieje szczególna podstawa prawna, na którą administrator może się powołać, aby kontynuować gromadzenie określonych danych. W przypadku umowy zawierającej spersonalizowaną ofertę przygotowaną na podstawie zachowania kierowcy, może to oznaczać, że w rezultacie powinno nastąpić przywrócenie standardowych warunków umowy w odniesieniu do danego użytkownika. Takie funkcje powinny być wdrożone w pojeździe, choć mogłyby zostać również udostępnione osobom, których dane dotyczą, za pośrednictwem dodatkowych środków (np. specjalnej aplikacji). Ponadto, aby umożliwić osobom, których dane dotyczą, szybkie i łatwe usunięcie danych osobowych, które mogą być przechowywane w desce rozdzielczej samochodu (np. dane dotyczące historii GPS, przeglądania stron internetowych itp.), EROD zaleca, by producenci zapewniali prostą funkcjonalność (jak np. przycisk usuwania).

92. Sprzedaż pojazdu podłączonego do internetu i związana z tym zmiana właściciela powinna również pociągać za sobą usunięcie wszelkich danych osobowych, które nie są już potrzebne do wcześniej określonych celów, a osoba, której dane dotyczą, powinna mieć możliwość skorzystania z prawa do przeniesienia danych.

2.7 Bezpieczeństwo

93. Producenci pojazdów i sprzętu, dostawcy usług i inni administratorzy danych powinni wprowadzić środki gwarantujące bezpieczeństwo i poufność przetwarzanych danych oraz wdrożyć wszelkie użyteczne środki ostrożności, aby zapobiec przejęciu kontroli przez osobę nieuprawnioną. W szczególności przedstawiciele branży powinni rozważyć wprowadzenie następujących środków:

- szyfrowanie kanałów komunikacyjnych za pomocą najnowocześniejszego algorytmu;
- system zarządzania kluczami kryptograficznymi, które są niepowtarzalne dla każdego pojazdu, a nie dla każdego modelu;
- w przypadku zdalnego przechowywania danych – szyfrowanie takich danych za pomocą najnowocześniejszych algorytmów;
- regularne odnawianie kluczy kryptograficznych;
- ochrona kluczy kryptograficznych przed jakimkolwiek ujawnieniem;
- uwierzytelnianie urządzeń odbierających dane;
- zapewnianie spójności danych (np. poprzez haszowanie);
- uzależnienie dostępu do danych osobowych od niezawodnych technik uwierzytelniania użytkownika (hasło, certyfikat elektroniczny itp.).

94. Zwłaszcza w odniesieniu do producentów pojazdów EROD zaleca wprowadzenie następujących środków bezpieczeństwa:

- oddzielenie najważniejszych funkcji pojazdu od tych, które zawsze zależą od możliwości telekomunikacyjnych (np. informacyjno-rozrywkowych);
- wdrożenie środków technicznych umożliwiających producentom pojazdów szybkie usuwanie luk w zabezpieczeniach przez cały okres eksploatacji pojazdu;
- w przypadku najważniejszych funkcji pojazdu – należy w miarę możliwości w pierwszej kolejności korzystać z bezpiecznych środków łączności, które są przeznaczone specjalnie do transportu;

- utworzenie systemu alarmowego na wypadek ataku na systemy pojazdu, z możliwością działania w trybie awaryjnym[47];
- przechowywanie historii wszystkich zarejestrowanych przypadków dostępu do systemu informacyjnego pojazdu, np. sięgających maksymalnie sześciu miesięcy wstecz, aby umożliwić zrozumienie źródła ewentualnego ataku oraz okresowe przeprowadzanie przeglądu zarejestrowanych informacji w celu wykrycia ewentualnych nieprawidłowości.

95. Te ogólne zalecenia należy uzupełnić szczegółowymi wymogami, uwzględniając cechy i cel każdego przetwarzania danych.

2.8 Przekazywanie danych osobowych stronom trzecim

96. Zasadniczo tylko administrator danych i osoba, której dane dotyczą, mają dostęp do danych wygenerowanych przez pojazd podłączony do internetu. Administrator danych może jednak przekazywać dane osobowe partnerowi handlowemu (odbiorcy) w zakresie, w jakim takie przekazanie opiera się zgodnie z prawem na jednej z podstaw prawnych określonych w art. 6 RODO.

97. Ze względu na ewentualną wrażliwość danych dotyczących użytkowania pojazdu (np. odbyte podróże, styl jazdy) EROD zaleca, aby zgoda osoby, której dane dotyczą, była systematycznie uzyskiwana przed przekazaniem jej danych partnerowi handlowemu pełniącemu funkcję administratora danych (np. poprzez zaznaczenie pola, które nie jest domyślnie zaznaczone, lub, jeżeli jest to technicznie możliwe, poprzez użycie fizycznego lub logicznego urządzenia, do którego dana osoba ma dostęp z pojazdu). Wówczas to partner handlowy staje się odpowiedzialny za dane, które otrzymuje, i podlega wszystkim przepisom RODO.

98. Producent pojazdu, dostawca usług lub inny administrator danych może przekazać dane osobowe podmiotowi przetwarzającemu dane wybranemu w celu odegrania roli w świadczeniu usługi na rzecz osoby, której dane dotyczą, pod warunkiem że podmiot przetwarzający dane nie będzie wykorzystywał tych danych do celów własnych. Administratorzy danych i podmioty przetwarzające dane muszą sporządzić umowę lub inny dokument prawny określający obowiązki każdej ze stron i wyszczególniający przepisy art. 28 RODO.

2.9 Przekazywanie danych osobowych poza UE/EOG

99. W przypadku przekazywania danych osobowych poza Europejski Obszar Gospodarczy przewidziano specjalne zabezpieczenia zapewniające, aby przekazywane dane były objęte ochroną.

100. W efekcie administrator danych może przekazać dane osobowe odbiorcy tylko w zakresie, w jakim takie przekazanie jest zgodne z wymogami określonymi w rozdziale V RODO.

[47] Tryb awaryjny to tryb pracy pojazdu zapewniający działanie funkcji istotnych dla bezpiecznej eksploatacji pojazdu (tj. zgodnie z minimalnymi wymogami bezpieczeństwa), nawet jeśli inne, mniej ważne funkcje zostaną wyłączone (np. działanie urządzenia do nawigacji można uznać za nieistotne w przeciwieństwie do układu hamulcowego).

2.10 Korzystanie z technologii Wi-Fi w pojazdach

101. Postęp w dziedzinie technologii komórkowej umożliwił łatwe korzystanie z internetu podczas podróży. Choć uzyskanie łączności Wi-Fi w pojeździe jest możliwe przez hotspot w smartfonie lub specjalne urządzenie (klucz układu OBD-II, modem bezprzewodowy lub router itp.), większość producentów samochodów oferuje obecnie modele, które mają wbudowane łącze danych komórkowych i również mogą tworzyć sieci Wi-Fi. W zależności od przypadku należy uwzględnić różne aspekty:

Złączność Wi-Fi oferowana jako usługa przez zawodowego kierowcę, np. taksówkarza dla jego klientów. W takim przypadku kierowcę lub jego przedsiębiorstwo można uznać za dostawcę usług internetowych, a w związku z tym podlegają oni szczególnym obowiązkom i ograniczeniom w zakresie przetwarzania danych osobowych klientów;

Zusługa łączności Wi-Fi dostępna na wyłączny użytek kierowcy (kierowcy i jego pasażerów). W takim przypadku przetwarzanie danych osobowych uznaje się za działalność czysto osobistą lub domową zgodnie z art. 2 ust. 2 lit. c) i motywem 18 RODO.

102. Ogólnie upowszechnianie interfejsów sieciowych przez technologię Wi-Fi stwarza większe ryzyko dla prywatności osób fizycznych. Za pośrednictwem swoich pojazdów użytkownicy stają się bowiem ciągłymi nadawcami, a zatem mogą być identyfikowani i śledzeni. Aby zapobiec śledzeniu, producenci pojazdów i sprzętu powinni wprowadzić łatwe w obsłudze opcje rezygnacji, dzięki którym nie będzie pobierany identyfikator zestawu usług (SSID) pokładowej sieci Wi-Fi.

3 ANALIZY PRZYKŁADÓW

103. W niniejszej sekcji omówiono pięć konkretnych przykładów przetwarzania w kontekście pojazdów podłączonych do internetu, które to przykłady odpowiadają scenariuszom, z jakimi zainteresowane strony mogą mieć styczność w tym sektorze. Przykłady te obejmują przetwarzanie danych wymagające mocy obliczeniowej, która nie jest dostępna w samym pojeździe, lub przesyłania danych osobowych stronie trzeciej w celu przeprowadzenia dalszej analizy lub zdalnego uruchomienia dalszych funkcji. Dla każdego rodzaju przetwarzania w niniejszym dokumencie określono zamierzone cele, kategorie gromadzonych danych, okres zatrzymywania takich danych, prawa osób, których dane dotyczą, środki bezpieczeństwa, które należy wprowadzić, oraz odbiorców informacji. W przypadkach, w których niektóre z tych dziedzin nie zostały opisane w dalszej części dokumentu, zastosowanie mają zalecenia ogólne przedstawione w poprzedniej części.

104. Wybrane przykłady nie są wyczerpujące i mają na celu wskazanie różnorodności rodzajów przetwarzania, podstaw prawnych, podmiotów itp., które mogą być zaangażowane w kontekście pojazdów podłączonych do internetu.

3.1 Świadczenie usługi przez stronę trzecią

105. Osoby, których dane dotyczą, mogą zawrzeć umowę z dostawcą usług w celu uzyskania dostępu do usług o wartości dodanej związanych z ich pojazdem. Na przykład osoba, której dane dotyczą, może zawrzeć umowę ubezpieczenia opartą na użytkowaniu, która oferuje niższe składki ubezpieczeniowe za mniejszą liczbę przejechanych kilometrów („ile jeździsz, tyle płacisz”) lub dobre zachowanie kierowcy (ubezpieczenie uzależnione od stylu jazdy) i która wymaga monitorowania nawyków kierowców przez zakład ubezpieczeń. Osoba, której dane dotyczą, może również zawrzeć umowę z przedsiębiorstwem oferującym usługi awaryjnej pomocy drogowej, co wiąże się z przekazywaniem danych dotyczących lokalizacji pojazdu przedsiębiorstwu lub dostawcy usług w celu otrzymywania komunikatów lub ostrzeżeń o stanie pojazdu (np. ostrzeżenie o stopniu zużycia hamulców lub przypomnienie o terminie przeglądu technicznego).

3.1.1 Ubezpieczenie oparte na użytkowaniu

106. Mechanizm „ile jeździsz, tyle płacisz” jest rodzajem ubezpieczenia opartego na użytkowaniu, w ramach którego śledzi się liczbę przejechanych przez kierowcę kilometrów lub jego styl jazdy w celu rozróżnienia i nagrodzenia „bezpiecznych” kierowców poprzez przyznanie im niższych składek ubezpieczeniowych. Ubezpieczyciel będzie wymagał, aby kierowca zainstalował wbudowaną usługę telematyczną, tj. aplikację mobilną, lub aktywował wbudowany przy produkcji moduł, który śledzi pokonywane kilometry lub zachowanie kierowcy (sposób hamowania, gwałtowne przyspieszanie itp.), czyli ubezpieczającego. Informacje zebrane przez urządzenie telematyczne zostaną wykorzystane do przypisania kierowcy punktów w celu przeanalizowania, jakie ryzyko może on stanowić dla zakładu ubezpieczeń.

107. Ponieważ ubezpieczenie oparte na użytkowaniu wymaga zgody na podstawie art. 5 ust. 3 dyrektywy o e-prywatności, EROD podkreśla, że ubezpieczający musi mieć możliwość wyboru wykupienia polisy ubezpieczeniowej nieopartej na użytkowaniu. W przeciwnym razie zgody nie można byłoby uznać za wyrażoną dobrowolnie, ponieważ wykonanie umowy nie byłoby możliwe bez tej zgody. Ponadto zgodnie z art. 7 ust. 3 RODO wymaga się, aby osoba, której dane dotyczą, miała prawo wycofać zgodę.

3.1.1.1 Podstawa prawna

108. W przypadku gdy dane są gromadzone za pośrednictwem publicznie dostępnej usługi łączności elektronicznej (np. za pośrednictwem karty SIM znajdującej się w urządzeniu telematycznym), potrzebna będzie zgoda w celu uzyskania dostępu do informacji, które są już przechowywane w pojeździe, zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności. W istocie żadne z wyłączeń przewidzianych w tych przepisach nie może mieć zastosowania w tym kontekście: przetwarzanie nie odbywa się wyłącznie w celu przekazywania komunikatów za pośrednictwem sieci łączności elektronicznej ani nie jest związane z usługą społeczeństwa informacyjnego, wyraźnie zażądaną przez abonenta lub użytkownika. Zgodę można uzyskać w momencie zawierania umowy.

109. Jeżeli chodzi o przetwarzanie danych osobowych w następstwie przechowywania lub dostępu do urządzenia końcowego użytkownika końcowego, w tym konkretnym kontekście zakład ubezpieczeń może powołać się na art. 6 ust. 1 lit. b) RODO pod warunkiem, że jest w stanie wykazać, że przetwarzanie odbywa się w kontekście ważnej umowy zawartej z osobą, której dane dotyczą, oraz że przetwarzanie jest konieczne do wykonania tej umowy zawartej z daną osobą, której dane dotyczą. O ile przetwarzanie danych jest obiektywnie konieczne do wykonania umowy zawartej z daną osobą, której dane dotyczą, EROD uważa, że powołanie się na art. 6 ust. 1 lit. b) RODO nie skutkowałoby w tym konkretnym przypadku ograniczeniem dodatkowej ochrony przewidzianej w art. 5 ust. 3 dyrektywy o e-prywatności. Ta podstawa prawna urzeczywistniła się poprzez zawarcie przez osobę, której dane dotyczą, umowy z zakładem ubezpieczeń.

3.1.1.2 Gromadzone dane

110. Istnieją dwa rodzaje danych osobowych, które należy uwzględnić:

- **dane handlowe i dotyczące transakcji**: dane identyfikacyjne osoby, której dane dotyczą, dane dotyczące transakcji, dane dotyczące środków płatniczych itp.;
- **dane dotyczące użytkowania**: dane osobowe generowane przez pojazd, styl jazdy, dane dotyczące lokalizacji itp.

111. EROD zaleca, aby w miarę możliwości oraz uwzględniając ryzyko, że dane gromadzone za pośrednictwem skrzynki telematycznej mogłyby zostać niewłaściwie wykorzystane do stworzenia dokładnego profilu ruchów kierowcy, surowe dane dotyczące zachowania kierowcy były przetwarzane:

- wewnątrz pojazdu w skrzynkach telematycznych lub w smartfonie użytkownika, tak aby ubezpieczyciel miał dostęp wyłącznie do danych dotyczących wyników (np. liczby punktów przyznanych za styl jazdy), a nie do szczegółowych surowych danych (zob. sekcja 2.1);

- lub przez dostawcę usług telematycznych w imieniu administratora (zakładu ubezpieczeń) w celu wygenerowania wyników liczbowych, które są przekazywane do zakładu ubezpieczeń na określonej podstawie. W takim przypadku należy oddzielić surowe dane i dane bezpośrednio odnoszące się do tożsamości kierowcy. Oznacza to, że dostawca usług telematycznych otrzymuje dane w czasie rzeczywistym, ale nie zna imion i nazwisk, tablic rejestracyjnych itp. ubezpieczających. Z drugiej strony ubezpieczyciel zna imiona i nazwiska ubezpieczających, ale otrzymuje jedynie punkty i całkowitą liczbę kilometrów, a nie surowe dane wykorzystane do uzyskania tych punktów.

112. Ponadto należy zauważyć, że jeżeli do celów wykonania umowy niezbędny jest tylko przebieg, nie można gromadzić danych dotyczących lokalizacji.

3.1.1.3 Okres przechowywania

113. W kontekście przetwarzania danych do celów wykonania umowy (tj. świadczenia usługi) ważne jest rozróżnienie między dwoma rodzajami danych przed określeniem ich odpowiednich okresów zatrzymywania:

- **dane handlowe i dotyczące transakcji:** dane te można przechowywać w aktywnej bazie danych przez cały okres obowiązywania umowy. Po zakończeniu okresu umowy można je zarchiwizować w postaci fizycznej (na oddzielnym nośniku: DVD itp.) lub w sposób logiczny (poprzez zarządzanie uprawnieniami) na wypadek ewentualnych sporów. Następnie, po upływie ustawowych terminów przedawnienia, dane należy usunąć lub zanonimizować;

- **dane dotyczące użytkowania:** dane dotyczące użytkowania można sklasyfikować jako surowe dane i dane zagregowane. Jak wspomniano powyżej, jeśli to możliwe, administratorzy danych lub podmioty przetwarzające dane nie powinni przetwarzać surowych danych. Jeżeli okaże się to konieczne, surowe dane należy przechowywać wyłącznie przez okres niezbędny do opracowania danych zagregowanych oraz do potwierdzenia prawidłowości przeprowadzonego procesu agregacji. Dane zagregowane należy przechowywać tak długo, jak będzie to konieczne na potrzeby świadczenia określonej usługi, lub tak długo, jak będzie to wymagane z innych względów zgodnie z prawem Unii lub państwa członkowskiego.

3.1.1.4 Informacje, które należy przekazać osobom, których dane dotyczą, oraz prawa tych osób

114. Przed przystąpieniem do przetwarzania danych osobowych osobie, której dane dotyczą, należy w przejrzysty i zrozumiały sposób przekazać informacje wyszczególnione w art. 13 RODO. Osobę, której dane dotyczą, należy poinformować w szczególności o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu. W tym ostatnim przypadku EROD zaleca przyjęcie podejścia pedagogicznego, aby zwrócić uwagę na różnicę między surowymi danymi a wynikiem punktowym uzyskiwanym na ich podstawie, podkreślając – w razie potrzeby – że ubezpieczyciel będzie gromadził dane dotyczące wyniku punktowego wyłącznie w stosownych przypadkach.

115. Jeżeli dane nie są przetwarzane wewnątrz pojazdu, ale przez dostawcę usług telematycznych w imieniu administratora (zakład ubezpieczeń), w informacjach przekazywanych osobie, której dane dotyczą, warto wspomnieć o tym, że w takim przypadku dostawca usług nie będzie dysponował dostępem do danych bezpośrednio odnoszących się do tożsamości kierowcy (takich jak imiona i nazwiska, tablice rejestracyjne itp.). Ponadto, biorąc pod uwagę znaczenie poinformowania osób, których dane dotyczą, o konsekwencjach przetwarzania ich danych osobowych, a także to, że osoby, których dane dotyczą, nie powinny być zaskoczone faktem przetwarzania ich danych osobowych, EROD zaleca informowanie osób, których dane dotyczą, o zjawisku profilowania i wiążących się z nim konsekwencjach nawet

w przypadku, gdy nie wiąże się to z żadnym zautomatyzowanym podejmowaniem decyzji, o którym mowa w art. 22 RODO.

116. Jeżeli chodzi o prawa osób, których dane dotyczą, osoby te należy wyraźnie poinformować o dostępnych możliwościach w zakresie wykonywania przysługującego im prawa dostępu do danych, sprostowania danych, ograniczenia przetwarzania i usunięcia danych. Ponieważ surowe dane gromadzone w tym kontekście przekazuje osoba, której dane dotyczą (za pomocą określonych formularzy lub wskutek prowadzonej przez siebie działalności), i ponieważ dane te przetwarza się na podstawie art. 6 ust. 1 lit. b) RODO (wykonanie umowy), osoba, której dane dotyczą, jest uprawniona do skorzystania z przysługującego jej prawa do przenoszenia danych. Jak podkreślono w wytycznych dotyczących prawa do przenoszenia danych, EROD zdecydowanie zaleca, „aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, której dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych”[48].

117. Stosowne informacje można przekazać w chwili podpisania umowy.

3.1.1.5 Odbiorca:

118. EROD zaleca, aby – w miarę możliwości – dane dotyczące użytkowania pojazdu były przetwarzane bezpośrednio w skrzynkach telematycznych, tak aby ubezpieczyciel miał dostęp jedynie do danych dotyczących wyników (np. punktów), a nie do szczegółowych surowych danych.

119. Jeżeli dostawca usługi telematycznej gromadzi dane w imieniu administratora (zakładu ubezpieczeń) w celu wygenerowania wyników liczbowych, nie musi znać tożsamości kierowcy (np. danych dotyczących jego imienia i nazwiska, numerów tablic rejestracyjnych itp. ubezpieczających).

3.1.1.6 Bezpieczeństwo:

120. Obowiązują zalecenia ogólne. Zob. sekcja 2.7.

3.1.2 Wynajem i rezerwacja miejsca parkingowego

121. Właściciel miejsca parkingowego może chcieć je wynająć. W tym celu wskazuje lokalizację danego miejsca i ustala cenę jego wynajmu za pomocą aplikacji internetowej. Następnie, po wprowadzeniu miejsca parkingowego na listę, aplikacja przekaże jego właścicielowi powiadomienie w chwili, gdy kierowca wyrazi chęć jego zarezerwowania. Kierowca może wybrać lokalizację i sprawdzić ją pod kątem dostępności miejsc parkingowych w oparciu o szereg różnych kryteriów. Po potwierdzeniu przez właściciela transakcja zostaje zatwierdzona, a dostawca usług realizuję transakcję płatniczą, po czym kierowca udaje się we wskazane miejsce, korzystając z nawigacji GPS.

3.1.2.1 Podstawa prawna

122. W przypadku gromadzenia danych za pośrednictwem publicznie dostępnych usług łączności elektronicznej zastosowanie mają przepisy art. 5 ust. 3 dyrektywy o e-prywatności.

123. Ponieważ omawiana usługa jest usługą społeczeństwa informacyjnego, zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności otrzymanie zgody na uzyskanie dostępu do informacji, które są już przechowywane w pojeździe, nie jest wymagane, jeżeli abonent wyraźnie zażądał świadczenia danej usługi.

124. Do celów przetwarzania danych osobowych i wyłącznie w odniesieniu do danych niezbędnych do wykonania umowy, której osoba, której dane dotyczą, jest stroną, za podstawę prawną uznaje się art. 6 ust. 1 lit. b) RODO.

[48] Grupa Robocza Art. 29, Wytyczne dotyczące prawa do przenoszenia danych zgodnie z rozporządzeniem 2016/676, WP242 rev.01, zatwierdzone przez EROD, s. 13.

3.1.2.2 Gromadzone dane

125. Przetwarzane dane obejmują dane kontaktowe kierowcy (imię i nazwisko, adres e-mail, numer telefonu, typ pojazdu (np. samochód osobowy, samochód ciężarowy, motocykl), numer tablicy rejestracyjnej, okres parkowania, szczegółowe informacje dotyczące transakcji płatniczej (np. informacje na temat karty kredytowej)), a także dane nawigacyjne.

3.1.2.3 Okres przechowywania

126. Dane należy przechowywać jedynie tak długo, jak będzie to konieczne do wykonania umowy najmu miejsca parkingowego, lub tak długo, jak będzie to wymagane z innych względów zgodnie z prawem Unii lub państwa członkowskiego. Po upływie tego okresu dane są anonimizowane albo usuwane.

3.1.2.4 Informacje, które należy przekazać osobom, których dane dotyczą, oraz prawa tych osób

127. Przed przystąpieniem do przetwarzania danych osobowych osobie, której dane dotyczą, należy w przejrzysty i zrozumiały sposób przekazać informacje wyszczególnione w art. 13 RODO.

128. Osobę, której dane dotyczą, należy wyraźnie poinformować o dostępnych możliwościach w zakresie wykonywania przysługującego jej prawa dostępu do danych, sprostowania danych, ograniczenia przetwarzania i usunięcia danych. Ponieważ dane gromadzone w tym kontekście przekazuje osoba, której dane dotyczą (za pomocą określonych formularzy lub wskutek prowadzonej przez siebie działalności), i ponieważ dane te przetwarza się na podstawie art. 6 ust. 1 lit. b) RODO (wykonanie umowy), osoba, której dane dotyczą, jest uprawniona do skorzystania z przysługującego jej prawa do przenoszenia danych. Jak podkreślono w wytycznych dotyczących prawa do przenoszenia danych, EROD zdecydowanie zaleca, „aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, której dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych".

3.1.2.5 Odbiorca:

129. Zasadniczo prawo dostępu do danych przysługuje wyłącznie administratorowi danych oraz podmiotowi przetwarzającemu dane.

3.1.2.6 Bezpieczeństwo:

130. Obowiązują zalecenia ogólne. Zob. sekcja 2.7.

3.2 eCall

131. W razie poważnego wypadku, który nastąpił na terytorium Unii Europejskiej, pojazd automatycznie inicjuje system pokładowy eCall oparty na numerze 112, tj. na jednolitym europejskim numerze alarmowym (aby uzyskać bardziej szczegółowe informacje, zob. sekcja 1.1.), aby niezwłocznie wezwać karetkę pogotowia na miejsce wypadku zgodnie z rozporządzeniem (UE) 2015/758 z dnia 29 kwietnia 2015 r. w sprawie wymagań dotyczących homologacji typu na potrzeby wdrożenia systemu pokładowego eCall opartego na numerze alarmowym 112 oraz zmiany dyrektywy 2007/46/WE („rozporządzenie (UE) 2015/758").

132. Zainstalowany wewnątrz pojazdu generator eCall, umożliwiający przesłanie zgłoszenia eCall za pośrednictwem publicznych bezprzewodowych sieci łączności ruchomej, inicjuje połączenie alarmowe automatycznie w wyniku aktywacji czujników pokładowych albo ręcznie przez osoby znajdujące się w pojeździe wyłącznie w sytuacji, w której doszło do wypadku. Niezależnie od uruchomienia kanału audio drugim zdarzeniem inicjowanym automatycznie wskutek wypadku jest wygenerowanie minimalnego zbioru danych i przesłanie go do publicznego punktu przyjmowania zgłoszeń o wypadkach (PSAP).

3.2.1 Podstawa prawna

133. Jeżeli chodzi o stosowanie dyrektywy o e-prywatności, należy zwrócić uwagę na dwa przepisy:

- art. 9 odnoszący się do danych dotyczących lokalizacji innych niż dane o ruchu, który ma zastosowanie wyłącznie do usług łączności elektronicznej;
- art. 5 ust. 3 dotyczący uzyskiwania dostępu do informacji przechowywanych w generatorze zainstalowanym wewnątrz pojazdu.

134. Mimo że zgodnie z przywołanymi przepisami co do zasady konieczne jest uzyskanie zgody osoby, której dane dotyczą, w rozporządzeniu (UE) 2015/758 na administratora danych nałożono określony obowiązek prawny (osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić zgody na przetwarzanie jej danych). Dlatego też przepisy rozporządzenia (UE) 2015/758 mają charakter nadrzędny wobec konieczności uzyskania zgody kierowcy na przetwarzanie danych dotyczących lokalizacji i minimalnego zbioru danych[49].

135. Podstawą prawną przetwarzania takich danych będzie zgodność z obowiązkiem prawnym, o którym mowa w art. 6 ust. 1 lit. c) RODO (w tym przypadku rozporządzeniem (UE) 2015/758).

3.2.2 Gromadzone dane

136. Rozporządzenie (UE) 2015/578 stanowi, że dane przesyłane przez system pokładowy eCall oparty na numerze 112 zawierają tylko minimum informacji określonych w normie EN 15722:2015 „Inteligentne systemy transportowe – eBezpieczeństwo – eCall minimalne bazy danych", w tym:

- wskazanie, czy system eCall został uruchomiony ręcznie czy automatycznie;
- typ pojazdu;
- numer identyfikacyjny pojazdu (VIN);
- rodzaj napędu pojazdu;
- znacznik czasu wskazujący moment wygenerowania pierwotnej wiadomości zawierającej dane w ramach danego incydentu eCall;
- ostatnią znaną szerokość i długość geograficzną pojazdu ustaloną w ostatnim możliwym momencie poprzedzającym wygenerowanie wiadomości;
- ostatni znany rzeczywisty kierunek ruchu pojazdu ustalony w ostatnim możliwym momencie poprzedzającym wygenerowanie wiadomości (wyłącznie trzy ostatnie położenia pojazdu).

3.2.3 Okres przechowywania

137. Rozporządzenie (UE) 2015/758 stanowi, że dane nie są przechowywane dłużej, niż jest to konieczne do celów obsługi sytuacji nadzwyczajnych. Dane te usuwa się w pełni, gdy nie są już niezbędne do wspomnianego celu. Ponadto dane przechowywane w pamięci wewnętrznej systemu eCall usuwa się automatycznie w sposób ciągły. Dopuszcza się wyłącznie możliwość przechowywania informacji na temat trzech ostatnich położeń

[49] Należy zwrócić uwagę na fakt, że w art. 8 ust. 1 lit. f) mandatu negocjacyjnego Rady w sprawie wniosku dotyczącego rozporządzenia w sprawie e-prywatności przewidziano szczególne odstępstwo dla systemu eCall, ponieważ uzyskanie zgody nie jest konieczne w przypadku, gdy „konieczne jest zlokalizowanie urządzenia końcowego w sytuacji, w której użytkownik końcowy nawiąże połączenie alarmowe z jednolitym europejskim numerem alarmowym 112 albo z krajowym numerem alarmowym zgodnie z art. 13 ust. 3".

pojazdu, o ile dane te są ściśle niezbędne do określenia obecnego położenia i kierunku ruchu pojazdu w chwili zdarzenia.

3.2.4 Informacje, które należy przekazać osobom, których dane dotyczą, oraz prawa tych osób

138. Art. 6 rozporządzenia (UE) 2015/758 stanowi, że producenci są zobowiązani przekazywać jasne i wyczerpujące informacje w instrukcji pojazdu na temat przetwarzania danych dokonywanego przy korzystaniu z systemu eCall. Tego rodzaju informacje zawiera się w podręczniku użytkownika, oddzielnie dla systemu pokładowego eCall opartego na numerze 112 oraz dla jakiegokolwiek innego systemu eCall wykorzystującego usługi świadczone przez osoby trzecie, przed rozpoczęciem użytkowania danego systemu. Obejmują one:

- przywołanie podstawy prawnej przetwarzania;
- zapewnienie, że system pokładowy eCall oparty na numerze 112 uruchamia się domyślnie;
- warunki przetwarzania danych dokonywanego przez system pokładowy eCall oparty na numerze 112;
- konkretny cel przetwarzania danych w ramach eCall, który musi być ograniczony do sytuacji nadzwyczajnych, o których mowa w art. 5 ust. 2 akapit pierwszy rozporządzenia (UE) 2015/758;
- rodzaje zbieranych i przetwarzanych danych oraz odbiorców tych danych;
- termin zatrzymywania danych w systemie pokładowym eCall opartym na numerze 112;
- zagwarantowanie, że pojazd nie jest stale śledzony;
- warunki korzystania z praw przysługujących osobom, których dane dotyczą, oraz kontaktowania się ze służbami odpowiedzialnymi za obsługę wniosków dotyczących dostępu do danych;
- wszelkie niezbędne informacje dodatkowe dotyczące identyfikacji, śledzenia i przetwarzania danych osobowych w związku ze świadczeniem usług dostarczanych przez osobę trzecią (TPS) na potrzeby systemu eCall lub innych usług o wartości dodanej, które wymagają wyraźnej zgody właściciela i są zgodne z RODO. Należy w szczególności uwzględnić fakt, że mogą istnieć różnice między przetwarzaniem danych za pomocą systemu pokładowego eCall opartego na numerze 112 a przetwarzaniem danych za pomocą pokładowych systemów TPS eCall lub przy wykorzystaniu innych usług dodatkowych.

139. Ponadto dostawca usług jest również zobowiązany przekazać osobom, których dane dotyczą, informacje wyszczególnione w art. 13 RODO w przejrzysty i zrozumiały sposób. Osoby te należy w szczególności poinformować o celach przetwarzania danych osobowych, a także o tym, że przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

140. Ponadto, biorąc pod uwagę charakter przetwarzania, informacje o odbiorcach lub kategoriach odbiorców danych osobowych powinny być przejrzyste, a osoby, których dane dotyczą, powinny być informowane o tym, że danych nie udostępnia się żadnym podmiotom poza systemem pokładowym eCall opartym na numerze 112 przed momentem inicjowania zgłoszenia eCall.

141. Jeżeli chodzi o prawa osób, których dane dotyczą, należy zwrócić uwagę na fakt, że w takim przypadku nie mogą one skorzystać z przysługującego im prawa do sprzeciwu ani z prawa do przenoszenia danych, ponieważ przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego.

3.2.5 Odbiorca:

142. Danych nie udostępnia się żadnym podmiotom poza systemem pokładowym eCall opartym na numerze 112 przed momentem inicjowania zgłoszenia eCall.

143. Po jego zainicjowaniu (ręcznie przez osoby znajdujące się w pojeździe albo automatycznie w chwili wykrycia poważnej kolizji przez czujniki pokładowe) system eCall nawiązuje połączenie głosowe z odpowiednim PSAP i przesyła minimalny zbiór danych operatorowi PSAP.

144. Ponadto dane przekazywane za pomocą systemu pokładowego eCall opartego na numerze 112 i przetwarzane przez publiczne punkty przyjmowania zgłoszeń o wypadkach (PSAP) mogą być przekazywane służbom ratowniczym i partnerom usługi, o których mowa w decyzji nr 585/2014/UE, jedynie w przypadku zdarzeń związanych ze zgłoszeniami eCall i na warunkach określonych w tej decyzji i są wykorzystywane wyłącznie do realizacji celów tej decyzji. Dane przetwarzane przez PSAP dzięki systemowi pokładowemu eCall opartemu na numerze 112 nie są przekazywane żadnym innym osobom trzecim bez wyraźnej uprzedniej zgody osoby, której dotyczą te dane.

3.2.6 Bezpieczeństwo

145. W rozporządzeniu (UE) 2015/758 ustanowiono wymóg wyposażenia systemu eCall w technologie służące wzmocnieniu ochrony prywatności w celu zapewnienia użytkownikom właściwego poziomu ochrony prywatności, jak również niezbędnej ochrony przed inwigilacją i nadużyciami. Ponadto producenci powinni zapewnić, aby system pokładowy eCall oparty na numerze 112, jak również jakikolwiek inny system zapewniający funkcjonalność eCall opierający się na usługach świadczonych przez osoby trzecie lub na usługach dodatkowych był zaprojektowany w sposób uniemożliwiający wymianę danych osobowymi między tymi systemami.

146. Jeżeli chodzi o PSAP, państwa członkowskie powinny zapewnić ochronę danych osobowych przed nadużyciami, w tym bezprawnym dostępem, zmianami lub utratą, oraz dopilnować, aby na odpowiednim poziomie były ustanowione i należycie przestrzegane protokoły dotyczące przechowywania, czasu zatrzymywania, przetwarzania i ochrony danych osobowych.

3.3 Badania wypadkowości

147. Osoby, których dane dotyczą, mogą dobrowolnie zgodzić się na udział w badaniach wypadkowości służących zwiększeniu wiedzy na temat przyczyn wypadków drogowych oraz realizacji bardziej ogólnych celów naukowych.

3.3.1 Podstawa prawna

148. W przypadku gromadzenia danych za pośrednictwem publicznej usługi łączności elektronicznej zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności w celu uzyskania dostępu do informacji, które są już przechowywane w pojeździe, administrator będzie zobowiązany uzyskać zgodę osoby, której dane dotyczą. W istocie żadne z wyłączeń przewidzianych w tych przepisach nie może mieć zastosowania w tym kontekście: przetwarzanie nie odbywa się wyłącznie w celu przekazywania komunikatów za pośrednictwem sieci łączności elektronicznej ani nie jest związane z usługą społeczeństwa informacyjnego, wyraźnie zażądaną przez abonenta lub użytkownika.

149. Jeżeli chodzi o przetwarzanie danych osobowych, a także biorąc pod uwagę różnorodność i ilość danych osobowych niezbędnych do przeprowadzenia badań wypadkowości, EROD zaleca przetwarzanie danych po uzyskaniu uprzedniej zgody osoby, której dane dotyczą, zgodnie z art. 6 RODO. Taka uprzednia zgoda musi zostać udzielona na specjalnym formularzu, za pomocą którego osoba, której dane dotyczą, dobrowolnie zgadza się na udział w badaniu i przetwarzanie jej danych osobowych w tym celu. Zgoda musi być

wyrazem wolnej, sprecyzowanej i świadomej woli osoby, której dane podlegają przetwarzaniu (np. zaznaczenie pola, które nie było domyślnie oznaczone, lub skonfigurowanie komputera pokładowego w taki sposób, aby uruchomić odpowiednią funkcję w pojeździe). Zgoda taka musi zostać udzielona odrębnie i w konkretnym celu oraz nie może być połączona z umową nabycia lub leasingu nowego samochodu, a jej wycofanie musi być równie łatwe jak jej udzielenie. Wycofanie zgody skutkuje wstrzymaniem przetwarzania danych. Następnie dane usuwa się z aktywnej bazy danych lub poddaje się je anonimizacji.

150. Zgodę wymaganą zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności oraz zgodę potrzebną jako podstawę prawną dla przetwarzania danych można uzyskać jednocześnie (np. poprzez zaznaczenie pola wyraźnie wskazującego, na co osoba, której dane dotyczą, wyraża zgodę).

151. Należy zwrócić uwagę na fakt, że – w zależności od warunków przetwarzania (charakter administratora danych itp.) – dopuszcza się możliwość wyboru innej podstawy prawnej uzasadniającej przetwarzanie zgodnie z obowiązującymi przepisami, o ile taka podstawa prawna nie ogranicza zakresu dodatkowej ochrony zapewnianej na mocy art. 5 ust. 3 dyrektywy o e-prywatności (zob. pkt 15). Jeżeli przetwarzanie danych odbywa się zgodnie z inną podstawą prawną, np. jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit. e) RODO), EROD zaleca, aby osoby, których dane dotyczą, były dopuszczane do udziału w badaniu na zasadzie dobrowolności.

3.3.2 Gromadzone dane

152. Administrator danych gromadzi wyłącznie te dane osobowe, które są ściśle niezbędne do celów przetwarzania.

153. W tym kontekście bierze się pod uwagę dwa rodzaje danych:

- **dane dotyczące uczestników i pojazdów**;
- **dane techniczne z pojazdów** (prędkość chwilowa itp.).

154. Prowadzenie badań naukowych w dziedzinie wypadkowości uzasadnia gromadzenie danych na temat prędkości chwilowej, również przez osoby prawne, które nie świadczą usługi leżącej w interesie publicznym w ścisłym znaczeniu tego słowa.

155. Jak wspomniano powyżej, w opinii EROD dane na temat prędkości chwilowej gromadzone w kontekście badań wypadkowości nie są danymi związanymi z naruszeniem prawa, jeżeli chodzi o cel ich gromadzenia (tj. nie gromadzi się ich do celów związanych z prowadzeniem dochodzenia lub postępowania w sprawie naruszenia prawa), co uzasadnia ich gromadzenie przez osoby prawne, które nie świadczą usługi leżącej w interesie publicznym w ścisłym znaczeniu tego słowa.

3.3.3 Okres przechowywania

156. Należy dokonać rozróżnienia między dwoma rodzajami danych: po pierwsze danymi dotyczącymi uczestników i pojazdów, które można przechowywać przez cały okres prowadzenia badania, a po drugie danymi technicznymi z pojazdów, które powinny być przechowywane przez najkrótszy okres konieczny do zrealizowania zamierzonego cel. W tym kontekście okres pięciu lat od dnia zakończenia badania wydaje się rozsądny. Po upływie tego okresu dane należy usunąć lub zanonimizować.

3.3.4 Informacje, które należy przekazać osobom, których dane dotyczą, oraz prawa tych osób

157. Przed przystąpieniem do przetwarzania danych osobowych osobie, której dane dotyczą, należy w przejrzysty i zrozumiały sposób przekazać informacje wyszczególnione w art. 13 RODO. Osoby, których dane dotyczą, należy wyraźnie poinformować o fakcie gromadzenia danych, w szczególności w przypadku gromadzenia danych na temat prędkości chwilowej.

Ponieważ przetwarzanie danych odbywa się na podstawie zgody, osobę, której dane dotyczą, należy wyraźnie poinformować o przysługującym jej prawie do wycofania zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Co więcej, ponieważ dane gromadzone w tym kontekście przekazuje osoba, której dane dotyczą (za pomocą określonych formularzy lub wskutek prowadzonej przez siebie działalności), i ponieważ dane te przetwarza się na podstawie art. 6 ust. 1 lit. a) RODO (zgoda), osoba, której dane dotyczą, jest uprawniona do skorzystania z przysługującego jej prawa do przenoszenia danych. Jak podkreślono w wytycznych dotyczących prawa do przenoszenia danych, EROD zdecydowanie zaleca, „aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, której dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych". Dlatego też administrator danych powinien zapewnić osobie, której dane dotyczą, możliwość łatwego, swobodnego cofnięcia udzielonej zgody w dowolnym momencie, a także opracować narzędzia umożliwiające mu udzielanie odpowiedzi na wnioski w sprawie przeniesienia danych.

158. Takich informacji można udzielać po podpisaniu formularza o wyrażeniu zgody na udział w badaniu wypadkowości.

3.3.5 Odbiorca

159. Zasadniczo prawo dostępu do danych przysługuje wyłącznie administratorowi danych oraz podmiotowi przetwarzającemu dane.

3.3.6 Bezpieczeństwo

160. Jak wspomniano powyżej, stosowane środki bezpieczeństwa muszą być dostosowane do poziomu wrażliwości danych. Na przykład w przypadku gromadzenia danych na temat prędkości chwilowej (lub jakichkolwiek innych danych na potrzeby wydawania wyroków skazujących i prowadzenia postępowań w sprawie naruszenia prawa) w ramach badania wypadkowości, EROD zdecydowanie zaleca stosowanie solidnych środków bezpieczeństwa, takich jak:

- wdrażanie środków w zakresie pseudonimizacji (np. haszowanie danych takich jak nazwisko/imię osoby, której dane dotyczą, oraz numer seryjny przy użyciu klucza tajnego);
- przechowywanie danych dotyczących prędkości chwilowej i lokalizacji w odrębnych bazach danych (np. stosując najnowocześniejszy mechanizm szyfrowania wykorzystujący odrębne klucze i mechanizmy autoryzacji);
- lub usuwanie danych dotyczących lokalizacji niezwłocznie po sklasyfikowaniu zdarzenia referencyjnego lub referencyjnej sekwencji zdarzeń (np. rodzaj drogi, dzień/noc) oraz gromadzenie danych umożliwiających bezpośrednią identyfikację w odrębnej bazie danych dostępnej wyłącznie dla niewielkiej grupy osób.

3.4 Podejmowanie działań w przypadku kradzieży samochodu

161. Osoby, których dane dotyczą, mogą podjąć próbą znalezienia należącego do nich pojazdu w oparciu o dane dotyczące lokalizacji przypadku jego kradzieży. Możliwość korzystania z danych dotyczących lokalizacji jest ograniczona ścisłymi potrzebami prowadzonego dochodzenia i uzależniona od wyniku oceny przeprowadzonej przez właściwe organy ścigania.

3.4.1 Podstawa prawna

162. W przypadku gromadzenia danych za pośrednictwem publicznie dostępnej usługi łączności elektronicznej zastosowanie mają przepisy art. 5 ust. 3 dyrektywy o e-prywatności.

163. Ponieważ omawiana usługa jest usługą społeczeństwa informacyjnego, zgodnie z art. 5 ust. 3 dyrektywy o e-prywatności otrzymanie zgody na uzyskanie dostępu do informacji,

które są już przechowywane w pojeździe, nie jest wymagane, jeżeli abonent wyraźnie zażądał świadczenia danej usługi.

164. W przypadku przetwarzania danych osobowych za podstawę prawną przetwarzania danych dotyczących lokalizacji uznaje się zgodę udzieloną przez właściciela pojazdu lub, w stosownych przypadkach, konieczność wykonania umowy (wyłącznie w odniesieniu do danych niezbędnych do wykonania umowy, której właściciel pojazdu jest stroną).

165. Zgoda musi być wyrazem wolnej, sprecyzowanej i świadomej woli osoby, której dane podlegają przetwarzaniu (np. zaznaczenie pola, które nie było domyślnie oznaczone, lub skonfigurowanie komputera pokładowego w taki sposób, aby uruchomić odpowiednią funkcję w pojeździe). Swoboda wyrażenia zgody obejmuje możliwość jej cofnięcia w dowolnym momencie, o czym należy wyraźnie poinformować osobę, której dane dotyczą. Wycofanie zgody skutkuje wstrzymaniem przetwarzania danych. Następnie dane należy usunąć z aktywnej bazy danych, poddać je anonimizacji lub zarchiwizować.

3.4.2 Gromadzone dane

166. Dane dotyczące lokalizacji można przekazać wyłącznie w momencie zgłoszenia kradzieży – nie dopuszcza się możliwości ich gromadzenia w sposób ciągły przez cały okres postępowania.

3.4.3 Okres przechowywania

167. Dane dotyczące lokalizacji można przechowywać wyłącznie przez okres rozpoznawania sprawy przez właściwe organy prawne lub do chwili zakończenia postępowania mającego na celu rozwianie wątpliwości, która nie kończy się potwierdzeniem kradzieży pojazdu.

3.4.4 Informacje przeznaczone dla osób, których dane dotyczą

168. Przed przystąpieniem do przetwarzania danych osobowych osobie, której dane dotyczą, należy w przejrzysty i zrozumiały sposób przekazać informacje wyszczególnione w art. 13 RODO. Ściślej rzecz biorąc, EROD zaleca, aby administrator danych podkreślił, że nie dopuszcza się możliwości śledzenia pojazdu w sposób ciągły oraz że dane dotyczące lokalizacji można gromadzić i przekazać wyłącznie w chwili zgłoszenia kradzieży. Administrator jest ponadto zobowiązany przekazać osobie, której dane dotyczą, informacje o tym, że prawo dostępu do tych danych przysługuje wyłącznie upoważnionym funkcjonariuszom platformy zdalnego monitorowania elektronicznego.

169. Jeżeli chodzi o prawa osób, których dane dotyczą, w przypadku przetwarzania danych na podstawie uzyskanej zgody, osobę, której dane dotyczą, należy wyraźnie poinformować o przysługującym jej prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Ponadto z uwagi na fakt, że dane gromadzone w tym kontekście przekazuje osoba, której dane dotyczą (za pomocą określonych formularzy lub wskutek prowadzonej przez siebie działalności), i ponieważ dane te przetwarza się na podstawie art. 6 ust. 1 lit. a) (zgoda) lub art. 6 ust. 1 lit. b) (wykonanie umowy) RODO, osoba, której dane dotyczą, jest uprawniona do skorzystania z przysługującego jej prawa do przenoszenia danych. Jak podkreślono w wytycznych dotyczących prawa do przenoszenia danych, EROD zdecydowanie zaleca, „aby administratorzy danych wyraźnie wyjaśnili różnicę między rodzajami danych, jakie osoba, której dane dotyczą, może otrzymać na mocy przysługującego jej prawa dostępu i prawa do przenoszenia danych”.

170. Dlatego też administrator danych powinien zapewnić osobie, której dane dotyczą, możliwość łatwego, swobodnego cofnięcia udzielonej zgody (wyłącznie w przypadku, gdy zgoda stanowi podstawę prawną przetwarzania) w dowolnym momencie, a także opracować narzędzia umożliwiające mu udzielanie odpowiedzi na wnioski w sprawie przeniesienia danych.

171. Stosowne informacje można przekazać w chwili podpisania umowy.

3.4.5 Odbiorcy

172. W przypadku zgłoszenia kradzieży dane dotyczące lokalizacji można przekazać (i) upoważnionym funkcjonariuszom platformy zdalnego monitorowania elektronicznego oraz (ii) organom uprawnionym z mocy prawa.

3.4.6 Bezpieczeństwo

173. Obowiązują zalecenia ogólne. Zob. sekcja 2.7.