GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH
W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

**17/PL**

**WP 252**

# Opinia nr 03/2017 dotycząca przetwarzania danych osobowych w ramach współpracujących inteligentnych systemów transportowych (C-ITS)

**Przyjęta dnia 4 października 2017 r.**

**Spis treści**

**Spis treści**

# 1 Wprowadzenie

Dokument pt. „Przetwarzanie danych osobowych w ramach C-ITS", sporządzony przez Grupę Roboczą ds. Ochrony Danych i Prywatności wchodzącą w skład platformy na rzecz współpracujących inteligentnych systemów transportowych (C-ITS), formalnie przedstawiono Grupie Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych („Grupa 29") dnia 10 lipca 2017 r.

Platforma na rzecz C-ITS stanowi inicjatywę Dyrekcji Generalnej ds. Mobilności i Transportu Komisji Europejskiej, której realizację rozpoczęto pod koniec 2014 r. od utworzenia wyspecjalizowanych grup roboczych, z których każda zajmuje się różnymi aspektami wdrażania C-ITS – począwszy od bezpieczeństwa, przez normalizację techniczną, aż po ochronę danych.

Celem dokumentu jest zapewnienie podstawowych informacji dotyczących przetwarzania danych osobowych w kontekście C-ITS oraz uzyskanie wskazówek od Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, aby zwiększyć poziom ochrony danych w ramach tych nowych rodzajów zastosowań.

Komisja zaprosiła Grupę 29 do uczestnictwa poprzez udział jej delegatów w szeregu spotkań przygotowawczych przed wydaniem niniejszej opinii.

Grupa 29 docenia możliwość uczestnictwa w dyskusji z odpowiednimi zainteresowanymi stronami już od wczesnego etapu opracowywania tej nowej koncepcji technologicznej i w związku z tym poruszy pewne problematyczne kwestie związane z ogólnym rozporządzeniem o ochronie danych (RODO), które będzie stanowiło ramy prawne obowiązujące w chwili wdrożenia rozwiązania C-ITS.

Grupa 29 z zadowoleniem przyjmuje najnowszą rezolucję w sprawie ochrony danych w pojazdach zautomatyzowanych i podłączonych do sieci przyjętą podczas Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności, która odbyła się w Hongkongu w dniach 25–29 września 2017 r., potwierdzając wymogi ustanowione w tej rezolucji.

# 2 Koncepcja C-ITS

C-ITS jest rozwiązaniem typu *peer-to-peer* służącym do wymiany danych między pojazdami a innymi obiektami infrastruktury drogowej (znakami drogowymi lub innymi nadawczymi/przyjmującymi stacjami bazowymi) bez interwencji operatora sieci.

Koncepcja systemu polega na tym, że poszczególne elementy mogą się wzajemnie bezpośrednio informować o własnym statusie (przetwarzając dane zgromadzone przez czujniki, w które są wyposażone), otrzymując w zamian podobne informacje, i tym samym umożliwiając stworzenie obrazu (w odniesieniu do każdego z tych elementu) stanu środowiska otaczającego pojazd lub obiekt infrastruktury. Na podstawie tych komunikatów oczekuje się możliwości ulepszenia prognoz dotyczących sytuacji w ruchu drogowym oraz poprawy w zakresie zapobieganiu wypadkom.

C-ITS opiera się na ciągłej transmisji. Generuje on doraźne komunikaty i nie wymaga nawiązywania stałej komunikacji lub stałych połączeń między poszczególnymi elementami.

W kontekście C-ITS wymieniane są dwa rodzaje komunikatów: tzw. komunikaty świadomości współpracy (ang. *Cooperative Awareness Messages, CAM*) nadawane w sposób ciągły, które zawierają dane kinematyczne i wymiary pojazdu, oraz zdecentralizowane wiadomości środowiskowe (ang. *Decentralised Environmental Notification Messages, DENM*) wysyłane oprócz komunikatów CAM wyłącznie w przypadku wystąpienia określonych zdarzeń (takich jak wypadki) w niecierpiących zwłoki sytuacjach nadzwyczajnych, które zawierają informacje dotyczące miejsca wystąpienia tego rodzaju zdarzenia.
Komunikaty CAM i DENM zawierają podpisy kryptograficzne, które gwarantują otrzymującej stronie, że komunikaty są wysyłane przez zaufanego nadawcę. Dystrybucja certyfikatów wśród poszczególnych elementów systemu odbywa się za pomocą architektury infrastruktury klucza publicznego. Infrastruktura klucza publicznego jest strukturą zarządzania, w ramach której każdy z certyfikatów w danej chwili jest jednoznacznie przypisany danemu pojazdowi. Certyfikat poświadcza, że jest on uznany przez system i godny zaufania.

W strategii na rzecz C-ITS Komisja Europejska wskazała już szereg przypadków użycia dotyczących wstępnego wdrożenia (zastosowania od pierwszego dnia). Przypadki te, jak określono w dokumencie sporządzonym przez Grupę Roboczą ds. Ochrony Danych i Prywatności zajmującą się C-ITS, są w większości związane z funkcjami informacyjnymi (takimi tak ostrzeżenia o robotach drogowych, informacje o warunkach pogodowych itp.). W tych przypadkach kierowca zachowuje pełną kontrolę nad pojazdem i ponosi odpowiedzialność za działania pojazdu. W perspektywie długookresowej oraz przy zwiększonym poziomie automatyzacji oczekuje się wzrostu wpływu C-ITS, ponieważ system ten może stopniowo przejmować od kierowcy funkcję podejmowania decyzji dotyczących prowadzenia pojazdu.

Grupa 29 skoncentruje się wyłącznie na tych wstępnych możliwościach zastosowań C-ITS. Wprowadzenie wyższych poziomów automatyzacji spowoduje pojawienie się nowych, wysoce istotnych kwestii dotyczących wpływu na wolności i prawa obywateli Unii. Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, a w dalszej perspektywie również Europejska Rada Ochrony Danych, ocenią te kwestie na późniejszym etapie. Grupa 29 chciałaby przy tej okazji zachęcić do podjęcia w odpowiednim terminie dialogu między odpowiednimi zainteresowanymi stronami, dotyczącego wpływu tych ewolucyjnych scenariuszy na ochronę danych, z uwzględnieniem również skomplikowanych kwestii etycznych związanych z tego rodzaju nową, głęboką interwencją w działania, którymi tradycyjnie zarządzał człowiek.

# 3 Streszczenie dokumentu roboczego dotyczącego C-ITS

## *3.1 Dane osobowe*

Grupa Robocza ds. Ochrony Danych i Prywatności zajmująca się współpracującymi inteligentnymi systemami transportowymi przyznaje, że komunikaty wymieniane przez pojazdy stanowią dane osobowe. Co do zasady wniosek ten wynika z dwóch spostrzeżeń: 1) komunikaty zawierają certyfikaty autoryzacyjne wydane przez infrastrukturę klucza publicznego, jednoznacznie przypisane do nadawcy; 2) komunikaty zawierają pozycję, znacznik czasu, dane dotyczące lokalizacji i wymiary pojazdu.

W dokumencie sklasyfikowano obowiązujący mechanizm służący do wymiany komunikatów CAM i DENM wraz z certyfikatami cyfrowymi jako przetwarzanie danych pseudonimicznych, argumentując, że dodatkowe informacje (związek pomiędzy posiadaczem certyfikatu a danymi dotyczącymi pojazdu) są przechowywane osobno od użytkownika danych (informacje te są przechowywane przez organy certyfikacji). Zgodnie z art. 4 pkt 5 RODO, aby zidentyfikować osoby, których dane dotyczą, konieczne byłyby zatem dodatkowe informacje. Dlatego też w dokumencie stwierdzono, że należałoby zastosować art. 11 RODO (przetwarzanie niewymagające identyfikacji). W dokumencie nie odniesiono się jednak do przetwarzania dokonywanego przez organy certyfikacji ani nie podano szczegółów technicznych dotyczących infrastruktury klucza publicznego, które są niezbędne do zapewnienia, aby wymieniane dane były praktycznie pseudonimiczne.

## *3.2 Podstawa prawna*

Grupa Robocza ds. Ochrony Danych i Prywatności działająca w ramach platformy na rzecz C-ITS stwierdza, że zgodność z prawem przetwarzania nie może się opierać wyłącznie na jednej podstawie prawnej, lecz na połączeniu dwóch podstaw lub ich większej liczby, z uwzględnieniem harmonogramu oraz w celu wdrożenia nowej technologii w 2019 r. Podsumowując, Grupa Robocza ds. C-ITS uznaje, że biorąc pod uwagę charakter przedstawionych zastosowań od pierwszego dnia, właściwe mogłyby być następujące możliwe podstawy prawne lub ich połączenie:

- interes publiczny (art. 6 ust. 1 lit. e) RODO);
- wykonanie umowy (art. 6 ust. 1 lit. b) RODO);
- wyrażenie zgody (art. 6 ust. 1 lit. a) RODO);
- prawnie uzasadniony interes (art. 6 ust. 1 lit. f) RODO).

Grupa Robocza ds. C-ITS zauważa, że aby możliwe było zastosowanie interesu publicznego jako podstawy prawnej, konieczność tego rodzaju przetwarzana musi być przewidziana w prawie krajowym lub w prawie Unii. Można byłoby ją przewidzieć we wdrażaniu unijnej strategii na rzecz bezpieczeństwa ruchu drogowego, wydajności transportu i zrównoważenia środowiskowego. W dyrektywie 2010/40/UE w sprawie ITS zezwolono Komisji Europejskiej na przyjęcie wiążących specyfikacji w tej dziedzinie za pośrednictwem aktów delegowanych. Grupa Robocza ds. C-ITS uznaje obowiązkowe wdrożenie C-ITS za jeden z wariantów, jednak nie w odniesieniu do wstępnego wdrożenia w 2019 r.

Grupa Robocza ds. C-ITS rozważyła wariant przetwarzania danych osobowych, w przypadku gdy jest to konieczne do wykonania umowy, której stroną jest osoba, której dane dotyczą. Zgodnie z wnioskami wyciągniętymi przez Grupę Roboczą ds. C-ITS przedmiotowa podstawa prawna może nie mieć powszechnego zastosowania. Można oprzeć się na tej podstawie prawnej w szczególnych sytuacjach, na przykład jeżeli osoba, której dane dotyczą, faktycznie zawarła z prywatnym zarządcą drogi umowę, uprawniającą ją do poruszania się po tej drodze. Grupa Robocza ds. C-ITS zauważa, że istnieje łańcuch podmiotów uczestniczących w ramach C-ITS (obejmujący producentów samochodów, programistów, zarządców dróg). Mogą oni być współadministratorami, jak zdefiniowano w art. 26 RODO. Aby móc się opierać na podstawie prawnej dotyczącej konieczności wykonania umowy, należy przeprowadzić ocenę ról poszczególnych podmiotów w odniesieniu do celów i sposobów.

Jeżeli chodzi o podstawę prawną wyrażenia zgody, Grupa Robocza ds. C-ITS odnosi się do ograniczeń technicznych wynikających z nadawczego charakteru komunikatów. W ramach C-ITS podmioty pełniące rolę administratorów danych mogą nie pozostawać w bezpośredniej indywidualnej relacji z osobą, której dane dotyczą. Osoba, której dane dotyczą, nie jest i nie może być świadoma wszystkich odbiorców nadawanych przez siebie komunikatów,z uwagi na sposób opracowania normy [1]. Grupa Robocza ds. C-ITS sugeruje jednak możliwość dołączania do nadawanych komunikatów CAM i DENM znaczników, w których można zakodować preferencje użytkowników.

Grupa Robocza ds. C-ITS rozważyła również przetwarzanie do celów prawnie uzasadnionych interesów realizowanych przez administratora. Aby móc się opierać na tej podstawie prawnej, administrator danych musi zapewnić, by przetwarzanie nie naruszało interesów lub podstawowych praw i wolności osoby, której dane dotyczą. Jak wyraźnie przyznano w dokumencie, istnieje wiele ograniczeń utrudniających zastosowanie tej podstawy prawnej. Po pierwsze, jest to konieczność ustalenia, czyj interes jest realizowany w ramach łańcucha obowiązków C-ITS, oraz wykonanie potencjalnie odrębnych testów równowagi przez każdy z zaangażowanych podmiotów w zależności od pełnionych przez nie ról, a po drugie – wprowadzenie dodatkowych specjalnych zabezpieczeń w celu ograniczenia nadmiernego wpływu na osoby, których dane dotyczą.

# 4 Opinia Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych

## *4.1 Ramy prawne*

Wstępne wdrożenie współpracujących inteligentnych systemów transportowych jest planowane na 2019 r. Właściwe ramy prawne przetwarzania danych osobowych w odniesieniu do C-ITS stanowi zatem rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), które weszło w życie dnia 25 maja 2016 r. i będzie miało zastosowanie do dnia 25 maja 2018 r.

Ponadto w przyszłości istotne może być nowe rozporządzenie o prywatności i łączności elektronicznej. Zgodnie z wnioskiem Komisji Europejskiej (COM(2017) 10) [2] łączność maszyna-maszyna powinna być objęta zakresem stosowania tego rozporządzenia.

## *4.2 Dane osobowe / identyfikacja osób, których dane dotyczą*

Grupa Robocza ds. C-ITS poprawnie ustaliła, że dane przekazywane za pośrednictwem C-ITS stanowią dane osobowe, ponieważ odnoszą się do zidentyfikowanych lub możliwych do zidentyfikowania osób, których dane dotyczą. Osoby, których dane dotyczą, można identyfikować na różne sposoby. Pierwszym sposobem są certyfikaty dostarczane w ramach

[1] ETSI EN 302 637-2 „Inteligentne systemy transportowe (ITS); Komunikacja pojazdowa; Podstawowy zestaw aplikacji; Część 2: Specyfikacja podstawowej usługi świadomości współpracy" oraz ETSI EN 302 637-3 „Inteligentne systemy transportowe (ITS); Komunikacja pojazdowa; Podstawowy zestaw aplikacji; Część 3: Specyfikacje podstawowej usługi powiadamiania w środowisku zdecentralizowanym".

[2] Wniosek ustawodawczy Komisji Europejskiej COM(2017) 10 w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej (rozporządzenie w sprawie prywatności i łączności elektronicznej), styczeń 2017 r. Zob. również opinia WP247 Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

infrastruktury klucza publicznego, ponieważ certyfikaty te będą niepowtarzalne z założenia, aby umożliwić jednoznaczne ustalenie tożsamości pojazdu, w którym są zainstalowane. Drugi sposób dotyczy samych danych dotyczących lokalizacji, ponieważ możliwości identyfikacyjne takich danych są powszechnie znane[3]: wystarczy zaledwie kilka punktów na trasie, aby z dużą precyzją wyodrębnić jednostkę w populacji, biorąc pod uwagę w większości regularne schematy przemieszczania się osób.

Dotyczy to w szczególności komunikatów CAM. Komunikaty DENM obejmują również bilety autoryzacyjne i dane opisujące konkretne zdarzenie. W zależności od okoliczności przebiegu zdarzenia (np. małej gęstości zaludnienia obszaru, szczególnej pory dnia lub dynamiki łańcucha wydarzeń) komunikaty te mogą również umożliwić identyfikację osoby, której dane dotyczą.

Jeżeli chodzi o stosowanie art. 11 RODO, Grupa 29 pragnie zgłosić następujące zastrzeżenia. Art. 11 stanowi, że istnieją operacje przetwarzania, w przypadku których identyfikacja osoby, której dane dotyczą, nie jest konieczna lub nie jest już konieczna, przy czym administrator nie jest zobowiązany do identyfikacji osoby, której dane dotyczą, wyłącznie po to, by zastosować się do RODO. Artykuł ten należy interpretować jako sposób egzekwowania „rzeczywistej" minimalizacji danych pozostający jednak bez uszczerbku dla wykonywania przez osoby, których dane dotyczą, przysługujących im praw. Wykonywanie tych praw należy umożliwić przy pomocy „dodatkowych informacji" dostarczonych przez osobę, której dane dotyczą. Powołując się na art. 11 RODO bez określenia, jakie dodatkowe dane są konieczne w celu umożliwienia identyfikacji osób, których dane dotyczą, uniemożliwia się *de facto* wykonywanie przez osoby, których dane dotyczą, przysługujących im praw (do dostępu, poprawiania, przenoszenia itd.). Dane pseudonimiczne z definicji są jednak danymi osobowymi (zob. art. 4 RODO), ponieważ odnoszą się do możliwej do zidentyfikowania osoby fizycznej (zob. w szczególności motyw 26 RODO).

Grupa 29 zachęca zatem Grupę Roboczą ds. C-ITS do składania wniosków dotyczących koncepcji „dodatkowych informacji", które można przekazywać w ramach tej nowej usługi, aby zapewnić skuteczność tego przepisu, biorąc przykładowo pod uwagę szczegółowe dane dotyczące pojazdu lub charakter danych dotyczących lokalizacji zapewniający znaczącą możliwość identyfikacji. Grupa Robocza odrzuca wszelką wykładnię art. 11, której celem jest ograniczenie odpowiedzialności administratora (administratorów) z tytułu wypełniania obowiązków w zakresie ochrony danych.

Dane osobowe przetwarzane za pośrednictwem C-ITS mogą również obejmować szczególne kategorie danych określone w art. 10 RODO związane z niezastosowaniem się do sygnalizacji świetlnej (na przykład „niezastosowanie się do sygnalizacji świetlnej / bezpieczeństwo na skrzyżowaniu" w dokumencie). Tego rodzaju szczególne kategorie danych mogą być przetwarzane w ramach C-ITS i transmitowane do innych pojazdów. Art. 10 RODO stanowi, że przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. W związku z tym należy zmienić zastosowania od pierwszego dnia, aby zapobiec gromadzeniu i transmitowaniu jakichkolwiek informacji, które mogą być objęte zakresem stosowania art. 10.

[3] Opinia 05/2014 w sprawie technik anonimizacji Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych:, WP X.

Grupa Robocza dostrzega szereg możliwości technicznych zminimalizowania ryzyka ponownej identyfikacji.

Po pierwsze, można poprawić politykę wydawania certyfikatów w ramach infrastruktury klucza publicznego. Dopóki certyfikat jest ważny, dopóty można zidentyfikować i śledzić pojazd, przy czym śledzenie bliskiego zasięgu stanowi istotny element projektu C-ITS. Śledzenie bliskiego zasięgu umożliwia ścisłe powiązanie przyczynowe warunków drogowych oraz pojazdów poruszających się na tym obszarze, a zatem jest uznawane za konieczne w celu umożliwienia funkcjonowania systemu i zastosowań. Aby zapobiec długotrwałemu śledzeniu, które nie jest kluczowe dla zapewnienia bezpieczeństwa ruchu drogowego, bilety autoryzacyjne są z czasem zmieniane. Chociaż Grupa Robocza ds. C-ITS podkreśla potrzebę niskiej częstotliwości zmian biletów autoryzacyjnych, aby ograniczyć zużycie certyfikatów i nie przeszkodzić łatwej identyfikacji zagrożeń i ostrzeżeń o kierowcach znajdujących się w pobliżu, Grupa 29 zaleca ostrożną ocenę możliwości wprowadzenia wyższej częstotliwości w celu ograniczenia ryzyka długotrwałego śledzenia.

Po drugie, należy dostosować częstotliwość nadawania komunikatów CAM.
Zgodnie z zaproponowanymi ustawieniami częstotliwości nadawania komunikatów CAM możliwe byłoby śledzenie pojazdów w zasięgu kilku metrów. Byłoby to możliwe na przykład wówczas, gdyby różne segmenty bardzo gęstych sekwencji punktów o określonym odniesieniu czasowym, które można zlokalizować na przykład na mapie, były „barwione" w różny sposób za pośrednictwem konkretnego certyfikatu (przyjmując, że każdy certyfikat uzyskuje wizualnie inny kolor). Wątpliwości budzi zawarte w dokumencie twierdzenie Grupy Roboczej ds. C-ITS, że „różnorodne barwienie" tych segmentów na mapie (tj. załączanie do nich różnych certyfikatów) uniemożliwiałoby obserwatorowi rekonstrukcję całej trasy pojazdu. Dane dotyczące mobilności są nierozerwalnie i silnie skorelowane oraz wysoce powtarzalne w odniesieniu do większości kierowców, przy czym w przypadku atakującego posiadającego środki i motywację nie należy uznać za nieracjonalną możliwości połączenia pozornie niespójnych segmentów na pełnej trasie. Ponadto w przypadku zmiany certyfikatu przez pojazd możliwe wciąż będzie powiązanie starego certyfikatu z nowym certyfikatem: każdy inny pojazd znajdujący się w pobliżu pojazdu zmieniającego certyfikat będzie mógł być świadkiem zniknięcia starego certyfikatu i pojawienia się nowego certyfikatu, a zatem będzie mógł je połączyć. Grupa Robocza ds. C-ITS powinna zająć się tą kwestią, aby zapobiec tego rodzaju korelacjom.

Po trzecie, Grupa 29 podkreśla znaczenie zasady minimalizacji danych dla łagodzenia ryzyka ponownej identyfikacji, również poprzez stosowanie środków zaradczych, takich jak uogólnianie lub dodawanie zakłóceń[4]. Można opracować tego rodzaju środki zaradcze w taki sposób, aby nie wpływały one na ogólny obraz stanu otoczenia i możliwość wykrycia nowego zagrożenia, ograniczając jednocześnie niepotrzebne narażenie lub długotrwałe śledzenie kierowcy. Należy zwrócić szczególną uwagę na uogólnianie właściwości statycznych pojazdów lub dodawanie do nich zakłóceń, aby zminimalizować ryzyko śledzenia poprzez nadanie charakterystycznych cech wyróżniających właściwościom pojazdu.

## *4.3 Zagrożenia dla prywatności*

Grupa 29 przyznaje, że koncepcja leżąca u podstaw C-ITS może przynieść korzyści kierowcom – zapewniając zwiększone poziomy użyteczności i informacji środowiskowej,

[4] Zob. przykłady w opinii 05/2014 w sprawie technik anonimizacji Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, WP216.

a także ogółowi społeczeństwa – zapewniając poprawę bezpieczeństwa ruchu drogowego i ochronę bezpieczeństwa innych kierowców oraz pieszych. Grupa 29 podkreśla jednak, że wdrożenie na dużą skalę tej nowej technologii, które będzie się wiązało z gromadzeniem i przetwarzaniem bezprecedensowych ilości danych dotyczących lokalizacji osób fizycznych w Europie, wiąże się z nowymi wyzwaniami dla praw podstawowych i ochrony danych osobowych oraz prywatności zarówno użytkowników, jak i innych osób fizycznych, których może dotyczyć ten proces.

Przede wszystkim sama koncepcja C-ITS wiąże się z ujawnianiem danych, do których ujawniania kierowcy nie byli przyzwyczajeni, dotyczących mianowicie tego, dokąd jeżdżą, oraz w jaki sposób prowadzą. Za pomocą urządzeń nadawczych i odbiorczych pojazdu tego rodzaju prywatne informacje zostaną w sposób publiczny przekazane każdemu poruszającemu się w pobliżu pojazdowi. Jest to forma rozpowszechnionego stałego śledzenia zachowania, które może wywołać nieprzyjemne uczucie potajemnej kontroli.

Brak przejrzystości stanowi kolejne poważne zagrożenie dla prywatności. Za pośrednictwem swoich pojazdów użytkownicy staną się stałymi nadawcami. Muszą mieć pełną wiedzę na temat zakresu przetwarzania, pozostałych elementów systemu, z którymi wymieniają dane w środowisku C-ITS (innych pojazdów, producentów samochodów, zarządców dróg, innych publicznych lub prywatnych podmiotów), oraz sposobu, w jaki przetwarzają te dane.

Wybór transmisji wśród elementów systemu jako sposobu przekazywania komunikatów zamiast indywidualnej komunikacji stanowi kolejne wyzwanie: komunikaty mogą być odbierane przez nieograniczoną liczbę podmiotów, których zamiary i możliwości technologiczne nie są i nie mogą być znane nadawcy. Powoduje to asymetrię informacyjną pomiędzy nadawcami a pozostałymi elementami (odbiorcami) C-ITS. Należy wyrównać tę asymetrię, stosując wyższy poziom kontroli nad danymi osobowymi.

Dane kinematyczne i dane dotyczące lokalizacji będą bardzo wartościowe dla wielu zainteresowanych stron, które mają różne zamiary i cele, od reklamodawców do producentów samochodów i zakładów ubezpieczeń. Nieograniczony i powszechny dostęp do danych udostępnianych w ramach C-ITS może umożliwić nieuzasadnione nagromadzenie profilów przemieszczeń, stanowiących zbiory zarejestrowanych danych dotyczących prowadzenia pojazdów, na podstawie których można tworzyć, reklamować i sprzedawać spersonalizowane towary i usługi.

Dane dotyczące mobilności mogą być również atrakcyjne dla organów ścigania i służb egzekwowania przepisów drogowych, co wykracza poza zakres celów, dla których dane C-ITS są wytwarzane i przetwarzane. Taka sytuacja wzbudza obawy co do konieczności i proporcjonalności możliwego wykorzystywania tych danych we wspomnianych innych celach.

Innym znaczącym zagrożeniem dla ochrony danych związanym z C-ITS jest zmiana celu. Asymetria informacyjna dotycząca tożsamości pozostałych elementów systemu, która jest nieodłącznie związana z wybraną architekturą transmisji, może spowodować zniekształcenie pierwotnego zakresu komunikatów, przekierowując użytkowników w nieplanowane miejsca, jeżeli nie zastosuje się wobec tej asymetrii instrumentów budujących zaufanie. Takie zniekształcenie może wystąpić albo w wyniku nieprawidłowych prognoz stanu otoczenia (np. tworzenie zatorów komunikacyjnych zamiast ograniczenia obciążenia ruchem), albo wręcz na podstawie stronniczej interpretacji danych środowiskowych (np. zachęcanie użytkowników

do odwiedzania określonych obszarów w związku z interesami gospodarczymi jednego z elementów systemu).

## *4.4 Zgodność z prawem przetwarzania*

Warto podkreślić, że rozporządzenie (UE) 2016/679 nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze (art. 2 (2) (c)). Wyłączenie to może mieć zastosowanie tylko wtedy, gdy ogranicza się ono jedynie do przetwarzania, które odbywa się wewnątrz samochodu, i tylko wtedy, gdy kierowca ma pełną kontrolę nad przetwarzaniem w urządzeniu. Nie może mieć ono zastosowania wówczas, gdy urządzenie zainstalowane w samochodzie przekazuje dane innych samochodów znajdujących się w pobliżu, bez względu na to, czy odbywa się to natychmiastowo, czy w wyniku przetwarzania lokalnego. W takich przypadkach przetwarzanie nie ogranicza się do czynności o czysto osobistym charakterze.

Podstawą zgodności z prawem przetwarzania danych osobowych, które odbywa się w ramach funkcjonowania C-ITS, musi być art. 6 ust. 1 RODO. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

Ze względu na to, że celem zakresu C-ITS jest poprawa bezpieczeństwa ruchu drogowego, wspieranie skuteczności ruchu i promowanie zrównoważenia środowiskowego, również poprzez wdrożenie tego interoperacyjnego ogólnoeuropejskiego systemu, Grupa 29 stwierdza, że długoterminową podstawą prawną tego typu przetwarzania jest przyjęcie ogólnounijnego instrumentu prawnego (art. 6 ust. 1 lit. c) RODO). Ze względu na przewidywane rozpowszechnienie samochodów (pół)autonomicznych stosowanie tej technologii w pojazdach prawdopodobnie będzie kiedyś obowiązkiem porównywalnym z obowiązkiem prawnym producentów samochodów polegającym na stosowaniu funkcji eCall we wszystkich nowych pojazdach. Taki obowiązek prawny nie powinien umożliwiać powszechnego gromadzenia i przetwarzania danych osobowych. Należy właściwie ocenić zakres obowiązku prawnego oraz potwierdzić jego proporcjonalność i absolutną konieczność w demokratycznym społeczeństwie zgodnie z wymogami ochrony zapewnianej przez mające zastosowanie prawa podstawowe.

Komisja powinna jak najszybciej rozpocząć ten proces oceny i tworzenia prawa, aby uniemożliwić przetwarzanie danych dotyczących lokalizacji i innych danych osobowych obywateli Unii w ramach C-ITS bez podstawy prawnej i bez pełnego objęcia tej czynności odpowiednim stopniem ochrony.

W analizie pozostałych podstaw prawnych brakuje pewnych istotnych elementów. W tym celu pomocna może być ocena możliwości technicznych C-ITS i jego zakresu.

Istotą C-ITS jest śledzenie położenia pojazdu, jego prędkości i kierunku ruchu. Im częstsza jest wymiana komunikatów, tym dokładniejszy i bardziej szczegółowy obraz otoczenia pojazdów oraz tym lepsze możliwości systemu w zakresie wykrywania niebezpieczeństw. Grupa 29 zdaje sobie sprawę, że jednym z najważniejszych czynników w odniesieniu do funkcjonowania C-ITS jest poziom przyjęcia systemu i zapewniania danych; niski poziom zapewniania danych lub niska rozdzielczość obrazu otoczenia rejestrowanego przez każdy pojazd może wpłynąć na funkcjonalność C-ITS jako narzędzia zapewniającego bezpieczeństwo ruchu drogowego lub nawet ją zniweczyć.

Doprowadzenie do przyjęcia systemu nie oznacza jednak wymuszenia powszechnego śledzenia. Możliwość skorzystania z C-ITS powinna sama z siebie stanowić zachętę dla kierowców do dobrowolnego uczestnictwa w C-ITS. Wówczas możliwe będzie naturalne osiągnięcie krytycznej masy użytkowników niezbędnej do prawidłowego funkcjonowania systemu bez narzucania obowiązku jego stosowania przy jednoczesnym pozostawieniu swobody wyboru w kwestii uczestnictwa w systemie, a następnie – w przypadku zdecydowania się na korzystanie z systemu – wyboru parametrów śledzenia (czas, częstotliwość, lokalizacje), które są najlepiej dostosowane do preferencji danego użytkownika.

Poziom rozdzielczości śledzenia dobrze odzwierciedlają wskaźniki skuteczności systemu[5]:

„Pojazd będzie generować CAM co ok. 4 metry i przy zmianie kierunku jazdy o ponad 4°. W razie zmiany odległości między bieżącym a poprzednim położeniem o ponad 4 metry lub zmiany prędkości o ponad 0,5 m/s w porównaniu z ostatnią zarejestrowaną prędkością wysyłany jest komunikat CAM, przy czym odbywa się to co najmniej raz na sekundę i co najwyżej co 0,1 sekundy w normalnych warunkach".

Te parametry śledzenia stanowią model odniesienia. W dokumencie określono, że w rzeczywistości „stanowią one określoną obecnie specyfikację, która może się zmienić w zależności od faktycznych potrzeb nowych funkcji, jakie pojawią się w przyszłości". Ponadto zgodnie z dokumentem użytkownik nie może zmienić tych ustawień. W związku z tym Grupa Robocza ds. C-ITS zwraca uwagę na niewłaściwą równowagę między koniecznością wspierania przyjmowania C-ITS a koniecznością zapobiegania występowaniu „gapowiczów", którzy nie uczestniczą w systemie, ale czerpią z niego korzyści, przez ustalenie jak największej częstotliwości wymiany komunikatów (a tym samym szczegółowości śledzenia).

Grupa Robocza ds. C-ITS nie osiągnęła jak dotąd konsensusu na temat technicznych możliwości uzyskiwania zgody. Grupa Robocza podkreśla, że należy spełnić wszystkie warunki uzyskania ważnej zgody, o których mowa w art. 7 RODO i w motywie 42. Administratorzy danych muszą zwracać szczególną uwagę na warunki uzyskania konkretnej, dobrowolnej i świadomej zgody od różnych uczestników, takich jak właściciele lub użytkownicy samochodów. 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. Ponadto zgoda nie stanowi właściwej podstawy prawnej w odniesieniu do pracowników, ponieważ stosunek między pracodawcą

[5] Przetwarzanie danych osobowych w ramach C-ITS. Załącznik I – zastosowania od pierwszego dnia, normy i bezpieczeństwo (A.2.2 CAM).

a pracownikiem cechuje się zależnością prawną, a pracownicy nie mogą odmówić udzielenia zgody.

W szczególności ponieważ C-ITS opiera się na przekazie w trybie ciągłym, nie występuje moment braku ciągłości w przekazie, w którym możliwe byłoby zasygnalizowanie zamiaru lub woli po stronie użytkownika. Ponadto transmisja jest systemem komunikacji, w którym odbywa się ona tylko w jedną stronę i nie umożliwia reakcji, w związku z czym nie ma możliwości ustanowienia mechanizmu wzajemnego uznawania między osobą, której dane dotyczą (nadawcą), a administratorem danych (odbiorcą). Brak mechanizmu wzajemnego uznawania nie powinien sam z siebie uniemożliwiać zastosowania zgody, ale utrudnia wyłączne przetwarzanie danych do konkretnych i jasno określonych celów przez znanych administratorów danych. Z drugiej strony stwierdzenie zawarte w dokumencie, zgodnie z którym zgoda nie może zostać uznana za realną podstawę prawną, ponieważ na tym etapie administrator danych nie jest na tyle szczegółowo określony, aby osoba, której dane dotyczą, znała jego tożsamość, wprowadza w błąd: istnienie wyraźnie określonego administratora (lub administratorów) jest warunkiem wstępnym samego przetwarzania, a niejasności w zakresie jego identyfikacji nie może uzasadnić żadna podstawa prawna zgodna z art. 6 ust. 1 RODO. Działania techniczne, których celem jest uwzględnienie znaczników w strukturze komunikatów CAM i DENM sygnalizujących preferencje użytkowników, są dobrym punktem wyjścia, ale nadal nie stanowią rozwiązania.

Grupa Robocza ds. C-ITS odnosi się również do możliwości oparcia się na konieczności przetwarzania w celu wykonania umowy (art. 6 ust. 1 lit. b) RODO). Konkretna umowa zawarta między osobą, której dane dotyczą, a administratorem, odrębna od wszelkich innych umów o nabycie/leasing samochodu, może zasadniczo umożliwić kierowcom dobrowolne przystąpienie do systemu.

Jeżeli chodzi o możliwość zastosowania wariantu współadministratorów, o którym mowa w art. 26 RODO, warto podkreślić, że nie jest ona próbą sił współadministratorów ani nie ma na celu umożliwienia przyjęcia dowolnych ustaleń, których celem jest częściowe lub całkowite uchylenie się od obowiązków administratora. Współadministratorzy, którzy mają ustanowione stosunki z klientami lub osobami fizycznymi i mogą się z nimi bezpośrednio kontaktować, powinni wziąć całkowitą odpowiedzialność za informowanie ich o łańcuchu odpowiedzialności oraz o istnieniu i celach działań pozostałych współadministratorów.

Grupa 29 wielokrotnie wyjaśniała[6], że jeżeli przetwarzanie jest niezbędne do wykonania konkretnej i dowolnie wybranej umowy zawartej z osobą, której dane dotyczą, przepis ten należy interpretować ściśle, a między oceną konieczności a zgodnością z zasadą celowości istnieje wyraźny związek. W odniesieniu do C-ITS najważniejsze są dwa aspekty. Po pierwsze, należy z wyprzedzeniem wyraźnie ustalić strony umowy, aby zawęzić zakres przetwarzania do ograniczonego grona jedynie tych podmiotów, które wchodzą w zakres C-ITS, i aby uniknąć dalszego wykorzystania danych przez inne, nieokreślone osoby. Przedstawiony w dokumencie przykład umowy między osobami, których dane dotyczą, a prywatnym zarządcą drogi, jest niekompletny, ponieważ w przetwarzanie mogą być zaangażowane inne strony (np. producenci samochodów i deweloperzy oprogramowania), które działają albo jako współadministratorzy zgodnie z art. 26 RODO, albo jako całość w formie pojedynczego konsorcjum sprawującego rolę jedynego administratora, i które mogą zawrzeć umowy z osobami, których dane dotyczą. Po drugie przed samym przetwarzaniem należy stwierdzić zasadność umowy, jej istoty i celów, a administrator (administratorzy) musi

[6] Opinia 02/2013 w sprawie aplikacji na urządzenia inteligentne oraz opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE.

zbadać w odniesieniu do tej zasadności i celów, czy przetwarzanie danych jest niezbędne do wykonania umowy zawartej z każdym użytkownikiem, mając na uwadze, że samochodami mogą kierować ich właściciele lub inni użytkownicy.

Jeżeli chodzi o możliwość oparcia się na konieczności przetwarzania danych w uzasadnionym interesie (art. 6 ust. 1 RODO), Grupa 29 przypomina, że wariant ten nie powinien być traktowany jako „ostateczność" w skomplikowanych sprawach, w których trudno zastosować inne podstawy zgodności przetwarzania z prawem. Wynik testu równowagi może przesądzić o tym, czy art. 6 ust. 1 lit. f) RODO można traktować jako podstawę prawną przetwarzania. Jak stwierdzono w dokumencie, identyfikacja administratorów i ich interesów jest warunkiem wstępnym. Należy jednak wziąć pod uwagę również inne istotne czynniki[7]. W szczególności obejmują one: podstawę zasadności interesu (czy jest on zakorzeniony w interesie publicznym lub w interesie biznesowym konkretnej osoby), skutki dla osób, których dane dotyczą, ich oczekiwania dotyczące prywatności, również przy uwzględnieniu możliwego poufnego charakteru danych dotyczących lokalizacji, oraz dodatkowe zabezpieczenia (również z technicznego punktu widzenia), które mogą ograniczyć wszelkie nieuzasadnione skutki dla tych osób.

## *4.5 Ochrona*

C-ITS opiera się na transmisji komunikatów. W związku z tym zapewnienie poufności, integralności i dostępności komunikatów, tj. bezpieczeństwa komunikatów, wymaga dodatkowych działań i specyfikacji w porównaniu z komunikatami typu *one-to-one*.

Transmisja jest sposobem nieograniczonej komunikacji z nieskończoną liczbą odbiorców w zasięgu urządzenia emitującego. Zgodnie z powyższym każdy sensowny sposób, w jaki można ograniczyć przetwarzanie przekazywanych informacji wyłącznie do kontekstu stosowania C-ITS poprzez uniemożliwienie nienależnego przetwarzania przez pozostałych odbiorców niezwiązanych z C-ITS, będzie opierał się na istnieniu godnych zaufania elementów systemu oraz na założeniu, że korzystanie z danych pochodzących z C-ITS do celów innych niż bezpieczeństwo ruchu drogowego będzie stanowić przestępstwo.

Warto przypomnieć, że we wniosku ustawodawczym COM(2017) 10 dotyczącym rozporządzenia w sprawie prywatności elektronicznej przewidziano bardzo rygorystyczne ograniczenia w stosowaniu „emitowanych danych" takich jak komunikaty CAM i DENM, zaś w art. 8 ust. 2 określono ogólny zakaz stosowania, z wyjątkiem sytuacji, w której wykonuje się to wyłącznie przez czas niezbędny do ustanowienia połączenia i w celu jego ustanowienia oraz stosuje się właściwe środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa właściwy dla ryzyka, jak określono w art. 32 RODO.

W dokumencie położono szczególny nacisk na mechanizm infrastruktury klucza publicznego jako sposobu na zdobycie zaufania do systemu C-ITS. Co więcej, infrastruktura klucza publicznego ma na celu zapewnienie rozpowszechnienia określonego źródła informacji (w przypadku C-ITS są to certyfikaty cyfrowe) w ramach nadzorowanej struktury zarządczej. Infrastruktura klucza publicznego nie zapewnia żadnego mechanizmu egzekwowania, który może służyć do ustalenia prawdziwych zamiarów posiadaczy certyfikatów lub podmiotów certyfikujących. Niestety, ostatnio coraz częściej odnotowuje się zmowy lub incydenty

[7] Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE.

związane z bezpieczeństwem, które wpływają na organy certyfikacji; ponadto istnieje silna pokusa uzyskania certyfikatów wyłącznie w złej wierze[8].

Istnienie architektury infrastruktury klucza publicznego nie gwarantuje samo w sobie zaufania między elementami równorzędnymi. Aby wzmocnić zaufanie, niezbędne są inne dodatkowe środki. Ważnym elementem jest wdrożenie mechanizmów gwarantujących bezpieczeństwo. Inne istotne czynniki polegają na skrupulatnej i okresowej kontroli działań organów certyfikacji w formie kontroli krzyżowej między organami certyfikacji albo w formie audytów lub inspekcji przeprowadzanych przez instytucje publiczne, które uczestniczą w promocji C-ITS.

Zapewnienie integralności oznacza zapobieganie sytuacjom, w których dane mogą zostać zmienione w niedozwolony sposób, co doprowadziłoby do zakłócenia prawidłowego funkcjonowania systemu informacyjnego. W odniesieniu do transmisji w ramach C-ITS sytuacja taka może wystąpić, jeżeli elementy systemu (nawet te godne zaufania) manipulują obrazem otoczenia poprzez potajemne dostarczanie fałszywych danych lub realizują interesy biznesowe, a nie publiczny cel bezpieczeństwa ruchu drogowego. Filtrowanie wartości oddalonych w strumieniu komunikatów CAM i DENM, które może sygnalizować wystąpienie wskaźników odbiegających od średniej, jest istotnym mechanizmem zniechęcającym do wykorzystywania C-ITS w złej wierze oraz sposobem na zapewnienie, by wymieniano tylko te dane, która są niezbędne do osiągnięcia celu.

Dostępność to możliwość wykorzystania informacji w przewidzianym celu w razie wystąpienia takiej konieczności. Bardzo trudno jest zapewnić tę właściwość w otoczeniu nadawczym ze względu na konieczność znalezienia kompromisu pomiędzy czasem a jakością danych. Jeżeli istnienie (a tym samym dostępność) danych związanych z potencjalnym zagrożeniem jest generowane przez równoczesną, masową transmisję komunikatów na temat takiej sytuacji, opieranie się na zbyt małej próbie komunikatów może generować wiele fałszywych alarmów; z drugiej strony czekanie na zgromadzenie wystarczającej liczby dowodów z wielu różnych źródeł może trwać zbyt długo z perspektywy bezpieczeństwa ludzi. Zapobieganie wypadkom jest bardzo istotnym spodziewanym skutkiem przetwarzania danych osobowych w ramach C-ITS; Grupa 29 zaleca programistom, aby dołożyli szczególnej staranności i wszelkich starań w projektowaniu oprogramowania, które może odróżnić wyniki fałszywie dodatnie od wyników fałszywie ujemnych, również przez współpracę w aktualizacji parametrów usług, aby nie generować alarmów lub – przeciwnie – nie działać ze szkodą dla osób, których dane dotyczą, w razie wystąpienia prawdziwie niebezpiecznych sytuacji.

# 5 Wymagane działania

Grupa 29 z zadowoleniem przyjmuje starania podejmowane przez Komisję Europejską i Grupę Roboczą ds. Ochrony Danych i Prywatności w ramach platformy na rzecz współpracujących inteligentnych systemów transportowych w celu uwzględnienia zasad ochrony danych w funkcjonowaniu tych nowych zastosowań od samego początku.

Działania przeprowadzone przez Grupę Roboczą ds. C-ITS są dobrym punktem wyjścia, ale muszą zostać uzupełnione o szereg konkretnych działań podejmowanych na różnych poziomach. Grupa 29 uważa, że szczególnie ważne są następujące aspekty ochrony danych:

[8] Benjamin Edelman, *Adverse Selection in Online 'Trust' Certifications and Search Results*. „Electronic Commerce Research and Applications” 10, nr 1 (styczeń/luty 2011 r.).

- Komisja powinna wdrożyć sektorowe rozporządzenia w sprawie gromadzenia i przetwarzania danych w obszarze inteligentnych systemów transportowych;
- Komisja powinna określić plan działania w zakresie zgodnego z prawem przetwarzania danych dotyczących lokalizacji obywateli Unii w ramach zastosowań C-ITS, przy czym ostatecznym celem jest przyjęcie ogólnounijnego instrumentu prawnego (art. 6 ust. 1 lit. c) RODO);
- proces przyjmowania takiego instrumentu prawnego powinien się rozpocząć od oceny konieczności i proporcjonalności jego przepisów; ponadto w ramach procesu legislacyjnego należy zlecić przeprowadzenie oceny skutków w zakresie ochrony danych (art. 35 ust. 10 RODO), aby od samego początku sprecyzować ryzyko i środki łagodzące;
- pozostałe podstawy prawne przewidziane w dokumencie Grupy Roboczej ds. C-ITS (tzn. zgoda i realizacja uzasadnionego interesu wykonawcy) mogą służyć za podstawę tylko wtedy, gdy możliwe będzie rozwiązanie najważniejszych problemów określonych w niniejszej opinii w odniesieniu do każdej z tych podstaw;
- bez względu na wybraną podstawę prawną należy wyłączyć domyślne ustawienia wszystkich zainstalowanych funkcji C-ITS;
- należy wdrożyć przepisy art. 25 RODO (uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych), umożliwiając użytkownikom wybranie parametrów śledzenia (czas, częstotliwość, lokalizacje), które najlepiej odpowiadają ich preferencjom;
- należy zwiększyć bezpieczeństwo, aby ograniczyć ryzyko bezprawnego wykorzystania danych z C-ITS poza zakresem prawnie uzasadnionych celów;

- należy wprowadzić inne środki zaradcze uwzględniające ochronę prywatności już w fazie projektowania, takie jak generalizacja lub dodawanie zakłóceń, aby nie wpłynąć na ogólny obraz stanu otoczenia i możliwość wykrycia nowego zagrożenia, jednocześnie ograniczając zbędną ekspozycję lub długotrwałe śledzenie kierowcy;
- należy zwrócić szczególną uwagę na częstotliwość zmiany certyfikatów, aby zapewnić sprawiedliwą równowagę między wybraną częstotliwością a ryzykiem wynikającym z długotrwałego śledzenia;
- nie należy przekazywać szczególnych kategorii danych oraz danych związanych z wyrokami skazującymi i naruszeniami prawa;
- należy uważnie ocenić jakość danych, aby złagodzić wszelkie ryzyko nieobiektywnego zastosowania C-ITS, generowania fałszywych alarmów lub – przeciwnie – błędnej interpretacji faktycznych sytuacji nadzwyczajnych;
- należy publicznie i szczegółowo udokumentować i ściśle monitorować mechanizm infrastruktury klucza publicznego służący do dystrybucji certyfikatów, aby ograniczyć ryzyko zmowy między organami certyfikacji a elementami systemu lub ingerencji podmiotów działających w złej wierze;
- należy wyraźnie ustalić okresy zatrzymywania przetwarzanych danych przez wszystkie strony uczestniczące w platformie C-ITS oraz zakazać tworzenia scentralizowanej bazy danych wymienianych komunikatów przez wszelkie podmioty uczestniczące w C-ITS.